ProSecure Web/Email Security Threat Management Appliance STM150 Reference Manual

NETGEAR, Inc.
350 East Plumeria Drive
San Jose, CA 95134 USA

March 2009
202-10414-02
v1.1

Trademarks

NETGEAR and the NETGEAR logo are registered trademarks and ProSecure is a trademark of NETGEAR, Inc. Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Changes or modifications not expressly approved by the Netgear could void the user's authority to operate the equipment.

EU Regulatory Compliance Statement

The ProSecure Web/Email Security Threat Management Appliance STM150 is compliant with the following EU Council Directives: 89/336/EEC and LVD 73/23/EEC. Compliance is verified by testing to the following standards: EN55022 Class B, EN55024 and EN60950-1.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das ProSecure Web/Email Security Threat Management Appliance STM150 gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Certificate of the Manufacturer/Importer

It is hereby certified that the ProSecure Web/Email Security Threat Management Appliance STM150 has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the second category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference.

Read instructions for correct handling.

Additional Copyrights

AES	Copyright (c) 2001, Dr Brian Gladman <brg@gladman.uk.net>, Worcester, UK. All rights reserved. TERMS Redistribution and use in source and binary forms, with or without modification, are permitted subject to the following conditions: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. The copyright holder's name must not be used to endorse or promote any products derived from this software without his specific prior written permission. This software is provided 'as is' with no express or implied warranties of correctness or fitness for purpose.

Open SSL	Copyright (c) 1998-2000 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions * are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)” 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org. 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project. 6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)" THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).
MD5	Copyright (C) 1990, RSA Data Security, Inc. All rights reserved. License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function. License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work. RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind. These notices must be retained in any copies of any part of this documentation and/or software.

PPP	Copyright (c) 1989 Carnegie Mellon University. All rights reserved. Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by Carnegie Mellon University. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.
Zlib	zlib.h -- interface of the 'zlib' general purpose compression library version 1.1.4, March 11th, 2002. Copyright (C) 1995-2002 Jean-loup Gailly and Mark Adler. This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions: 1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required. 2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software. 3. This notice may not be removed or altered from any source distribution. Jean-loup Gailly: jloup@gzip.org; Mark Adler: madler@alumni.caltech.edu The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files ftp://ds.internic.net/rfc/rfc1950.txt (zlib format), rfc1951.txt (deflate format) and rfc1952.txt (gzip format)

Product and Publication Details

Model Number:	STM150
Publication Date:	March 2009
Product Family:	Threat Management Appliance
Product Name:	ProSecure Web/Email Security Threat Management Appliance STM150
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10414-02
Publication Version Number	1.1

Contents

About This Manual

Chapter 1
Introduction

Chapter 2
Provisioning Threat Management Services

About This Manual

The *NETGEAR® ProSecure™ Web/Email Security Threat Management Appliance STM150 Reference Manual* describes how to configure and troubleshoot a ProSecure Web/Email Security Threat Management Appliance STM150. The information in this manual is intended for readers with intermediate computer and networking skills.

Conventions, Formats, and Scope

The conventions, formats, and scope of this manual are described in the following paragraphs:

- **Typographical Conventions.** This manual uses the following typographical conventions:

Italic	Emphasis, books, CDs, file and server names, extensions
Bold	User input, IP addresses, GUI screen text
`Fixed`	Command prompt, CLI text, code
italic	URL links

- **Formats.** This manual uses the following formats to highlight special messages:

➡	**Note:** This format is used to highlight information of importance or special interest.

💡	**Tip:** This format is used to highlight a procedure that will save time or resources.

⚠	**Warning:** Ignoring this type of note may result in a malfunction or damage to the equipment.

⚠	**Danger:** This is a safety warning. Failure to take heed of this notice may result in personal injury or death.

- **Scope.** This manual is written for the threat management appliance according to these specifications:

Product	ProSecure Web/Email Security Threat Management Appliance STM150
Manual Publication Date	March 2009

For more information about network, Internet, firewall, and VPN technologies, see the links to the NETGEAR website in Appendix B, "Related Documents.".

➡	**Note:** Product updates are available on the NETGEAR, Inc. website at *http://kbserver.netgear.com/products/STM150.asp*.

Revision History

Manual Part Number	Manual Version Number	Publication Date	Description
202-10414-01	1.0	January 2009	First publication
202-10414-02	1.1	March 2009	Update to change product name, "heuristic scan" terminology changed to "distributed spam analysis", URL whitelists changed to now be case sensitive, correction of regulatory information, and various edits to improve clarity.

Chapter 1
Introduction

This chapter provides an overview of the features and capabilities of the ProSecure Web/Email Security Threat Management Appliance STM150. It also identifies the physical features of the appliance and the contents of its package.

Topics discussed in this chapter include:

- "What is the ProSecure Web/Email Security Threat Management Appliance STM150?" on page 1-1
- "Key Features and Capabilities" on page 1-2
- "What Can You Do with an STM150?" on page 1-3
- "Service Registration Card with License Key(s)" on page 1-4
- "Rear Panel Features" on page 1-5
- "Default IP Address, Login Name, and Password Location" on page 1-6
- "Choosing a Location for the STM150" on page 1-6

What is the ProSecure Web/Email Security Threat Management Appliance STM150?

The STM150 is an appliance-based, Web security solution that protects the network perimeter against Web-borne threats, from spyware, viruses, email, and blended threats. Ideally deployed at the gateway, it serves as the network's first line of defense against all types of threats and complements firewalls, IDS/IPS, dedicated intranet security products, and endpoint antivirus/anti-spyware software.

Powered by patent-pending stream scanning technology and backed by one of the most comprehensive malware databases in the industry, STM150 can detect and stop all known spyware and viruses at the gateway, preventing them from reaching your desktops and servers where cleanup would be much more difficult.

In addition to scanning HTTP, HTTPS, FTP, SMTP, POP3, and IMAP traffic, the STM150 protects networks against spam phishing attacks, and unwanted Web use.

About Stream Scanning

Stream scanning is based on the simple observation that network traffic travels in streams. The STM150 scan engine starts receiving and analyzing traffic as the stream enters the network. As soon as a number of bytes are available, scanning commences. The scan engine continues to scan more bytes as they become available, while at the same time another thread starts outputting the bytes that have been scanned.

This multi threaded approach, in which the receiving, scanning, and outputting processes occur concurrently, ensures that network performance remains unimpeded. The result is that the time to scan a file is up to five times faster than traditional antivirus solutions – a performance advantage that is easily noticeable to the end user.

Stream scanning also enables organizations to withstand massive spikes in traffic, as in the event of a malware outbreak.

Key Features and Capabilities

The STM150 is a true appliance that provides comprehensive protection against malware and uses real-time scanning technology to stop spyware, viruses, and other types of malware at the gateway, without stopping the Internet. This section highlights the STM150's primary features as a Web and Email security solution:

- **Real-time Protection** – The patent-pending stream scanning technology enables scanning of previously undefended real-time protocols, such as HTTP. Network activities susceptible to latency (for example, Web browsing) are no longer brought to a standstill.
- **Comprehensive Protection** – Provides both Web and email security, covering six major network protocols: HTTP, HTTPS, FTP, SMTP, POP3, and IMAP. The STM uses enterprise-class scan engines employing both signature-based and heuristic detection to stop both known and unknown threats. Malware database contains millions of signatures of spyware, viruses, and other malware.
- **Automatic Signature Updates** – Malware signatures are automatically updated on an hourly basis. Critical new signatures are typically deployed hours before they are available from other security vendors.
- **True Appliance** – Deploys in-line in a matter of minutes, anywhere in the network. Runs automatically and unobtrusively. Simply set and forget.

What Can You Do with an STM150?

The STM150 combines robust protection against malware with ease-of-use and advanced reporting and notification features to help you deploy and manage the device with minimal effort.

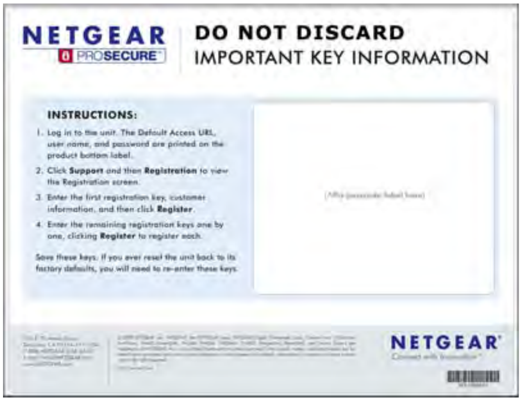
Here are some of the things that you can do with the STM150:

- **Scan Network Traffic for Malware** – Using the patent-pending stream scanning technology, you can configure the STM150 to scan HTTP, SMTP, POP3, HTTPS, IMAP, and FTP protocols. Unlike traditional batch-based scan engines that need to cache the entire file before they can scan, this scan engine checks traffic as it enters the network, ensuring unimpeded network performance.
- **Protect the Network Instantly** – the STM150 is a plug-and-play security solution that can be instantly added to networks without requiring network reconfiguration.
- **Receive Real-time Alerts and Generate Comprehensive Reports** – You can configure the STM150 to send out alerts whenever a malware or an outbreak is detected on the network. Real-time alerts can be sent out via email, allowing you to monitor malware events wherever you are.

  By configuring the STM150 to send out malware alerts, you can isolate and clean the infected computer before the malware incident can develop into a full blown outbreak. The STM150 also provides comprehensive reports that you can use to analyze network and malware trends.
- **SNMP Support** – You can enable and configure the STM150’s SNMP settings to receive SNMP traps through a supported MIB browser.
- **Automated Component Updates** – Downloading components regularly is the key to ensuring updated protection against new threats. The STM150 makes this administrative task easier by supporting automatic malware pattern, program and engine updates.

Service Registration Card with License Key(s)

Be sure to store the license key card that came with your unit in a secure location. You will need these keys to activate your product during the initial setup, and if you ever have to reset the unit back to its factory defaults.



NETGEAR PROSECURE

DO NOT DISCARD
IMPORTANT KEY INFORMATION

INSTRUCTIONS:

1. Log in to the unit. The Default Access URL, user name, and password are printed on the product bottom label.
2. Click **Support** and then **Registration** to view the Registration screen.
3. Enter the first registration key, customer information, and then click **Register**.
4. Enter the remaining registration keys one by one, clicking **Register** to register each.

Save these keys. If you ever reset the unit back to its factory defaults, you will need to re-enter these keys.

NETGEAR
Connect with Innovation™

Figure 1-1

Front Panel Features

The ProSecure Web/Email Security Threat Management Appliance STM150 front panel shown below includes two groups of RJ-45 connectors and status indicator light-emitting diodes (LEDs), including Power and Test lights:

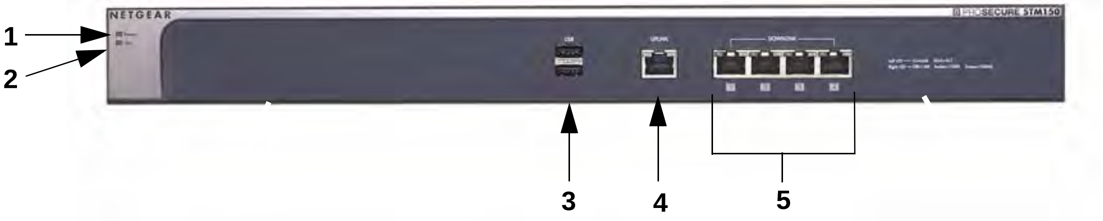


Figure 1-2

1. Power status

2. Power on test status

3. USB ports

4. Uplink switched N-way automatic speed negotiating auto MDI/MDIX Ethernet port

5. Downlink Ethernet ports
Four switched N-way automatic speed negotiating auto MDI/MDIX Ethernet ports.

Rear Panel Features

The STM150 rear panel functions are described below:

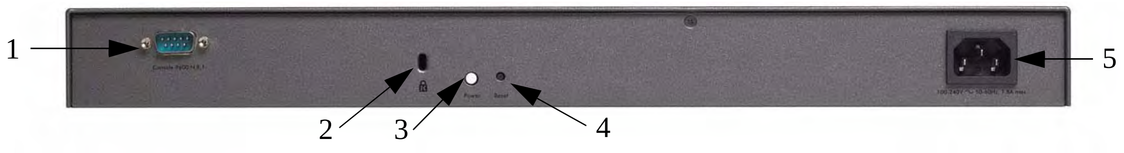


Figure 1-3

1. Console port: To connect to a COM port on a Microsoft Windows or Linux computer; may be used to perform the initial configuration.
2. Kensington Lock: Attach a kensington lock to prevent unauthorized removal of the unit.
3. Restart: Press to restart the unit; it does not reset the appliance to its factory defaults.
4. Reset: Use a sharp object, press and hold this button for about ten seconds until the front panel Test light flashes to reset the unit to factory default settings.

➡	**Note:** If you reset the unit, all configuration settings will be lost, the default password will be restored, and you will need to re-register the product license.

5. Power socket.

Default IP Address, Login Name, and Password Location

Check the label on the bottom of the STM150's enclosure if you need a reminder of the following factory default information:

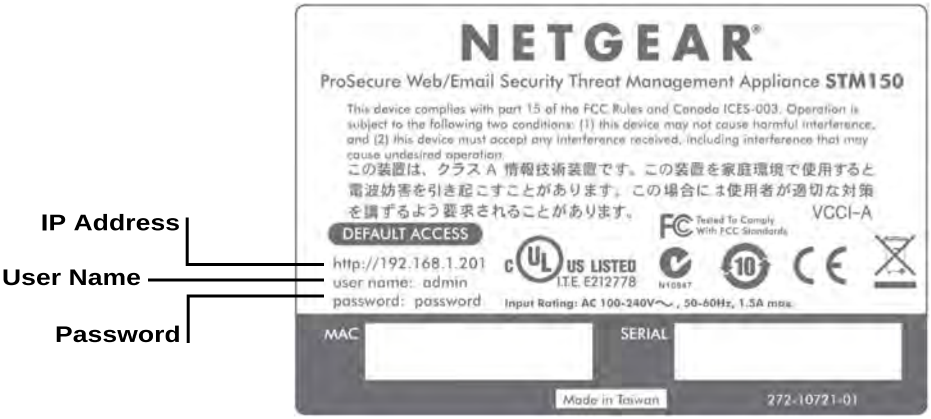

IP Address
User Name
Password
NETGEAR®
ProSecure Web/Email Security Threat Management Appliance STM150
This device complies with part 15 of the FCC Rules and Canada ICES-003. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
この装置は、クラスA 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。
VCCI-A
Tested To Comply With FCC Standards
DEFAULT ACCESS
http://192.168.1.201
user name: admin
password: password
c UL US LISTED
I.T.E. E212778
N10947
10
CE
Input Rating: AC 100-240V~, 50-60Hz, 1.5A max
MAC
SERIAL
Made in Taiwan
272-10721-01

Figure 1-4

Choosing a Location for the STM150

The STM150 is suitable for use in an office environment where it can be free-standing or mounted in a standard 19-inch equipment rack. Alternatively, you can rack-mount the STM150 in a wiring closet or equipment room. A mounting kit, containing two mounting brackets and four screws, is provided in the STM150 package.

When deciding where to position the STM150, ensure that:

- It is accessible and cables can be connected easily.
- Cabling is away from sources of electrical noise. These include lift shafts, microwave ovens, and air conditioning units.
- Water or moisture cannot enter the case of the unit.
- Airflow around the unit and through the vents in the side of the case is not restricted. Provide a minimum of 25 mm or 1 inch clearance.
- The air is as free of dust as possible.
- Temperature operating limits are not likely to be exceeded. Install the unit in a clean, air-conditioned environment. For information on the recommended operating temperatures for the STM150, refer to Appendix A, "Default Settings and Technical Specifications.

Using the Rack Mounting Kit

Use the provided mounting kit for the STM150 to install the appliance to a rack. The mounting brackets supplied with the STM150 are usually installed before the unit is shipped out. If the brackets are not yet installed, attach them using the supplied hardware.

Before mounting the STM150 in a rack, verify that:

- You have the correct screws (supplied with the installation kit)
- The rack onto which you will mount the STM150 is suitably located.

Chapter 2
Provisioning Threat Management Services

Provisioning the STM150 ProSecure Web/Email Security Threat Management Appliance STM150 in your network is described in this chapter.

This chapter contains the following sections:

Choosing a Deployment Scenario

The STM150 is an inline transparent bridge appliance that can easily be deployed to any point on the network without requiring network reconfiguration or additional hardware.

The following are the most common deployment scenarios for the STM150. Depending on your network environment and the areas that you want to protect, you can choose one or a combination of these deployment scenarios.

- "Gateway Deployment" on page 2-2
- "Server Group" on page 2-3
- "Segmented LAN Deployment." on page 2-4

Gateway Deployment

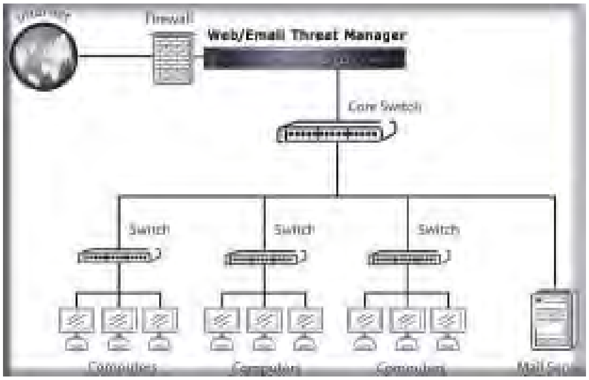


Figure 2-1

In a typical gateway deployment scenario, a single STM150 appliance is installed at the gateway – between the firewall and the LAN core switch – to protect the network against all malware threats entering and leaving the gateway. Installing the STM150 behind the firewall protects it from DoS attacks.

Server Group

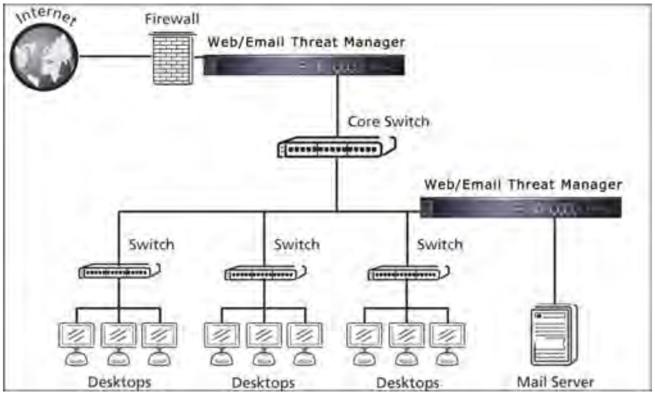


Figure 2-2

In a server group deployment, one STM150 appliance is installed at the gateway and another in front of the server group. This type of deployment helps split the network load and provides the mail server with dedicated protection against malware, including email-borne viruses and spam.

➡	**Note:** This configuration helps protect the mail server from internal as well as external clients.

Segmented LAN Deployment.

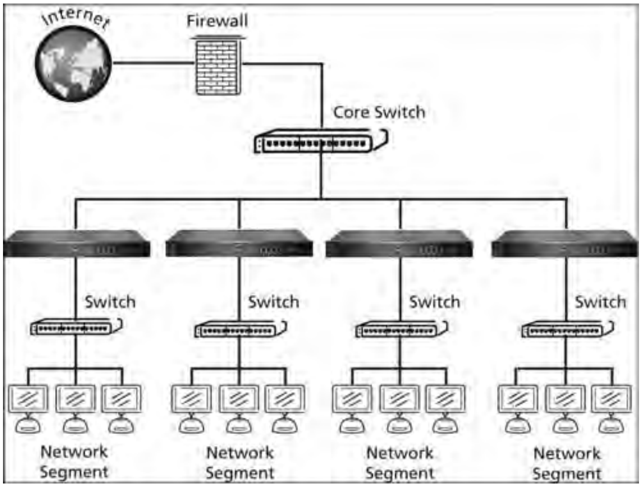


Figure 2-3

In a segmented LAN deployment, one STM150 appliance is installed in front of each network segment. This type of deployment helps split the network load and protects network segments from malware coming in through the gateway or originating from other segments.

⇨	**Note:** In segmented LAN deployment, VLAN is not supported; VLAN traffic cannot pass through the STM150.

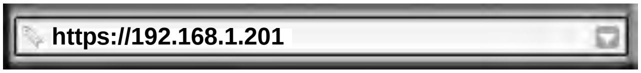
Use the Installation Guide to Perform Initial Configuration

Use the installation guide to perform the initial configuration of the STM150's basic system settings (for example, IP address, netmask, and DNS) so that it can function on the network. To perform the initial configuration, follow the instructions in the NETGEAR *Installation Guide, STM150*. The installation guide will walk you through connecting the unit, and using the setup wizard to complete the initial configuration. After using the setup wizard to complete the initial configuration, you can log in to make additional changes or to monitor the system using the steps below.

Logging In to the STM150

Follow these steps to log in to the STM150.

1. Use a browser to connect to https://192.168.1.201.

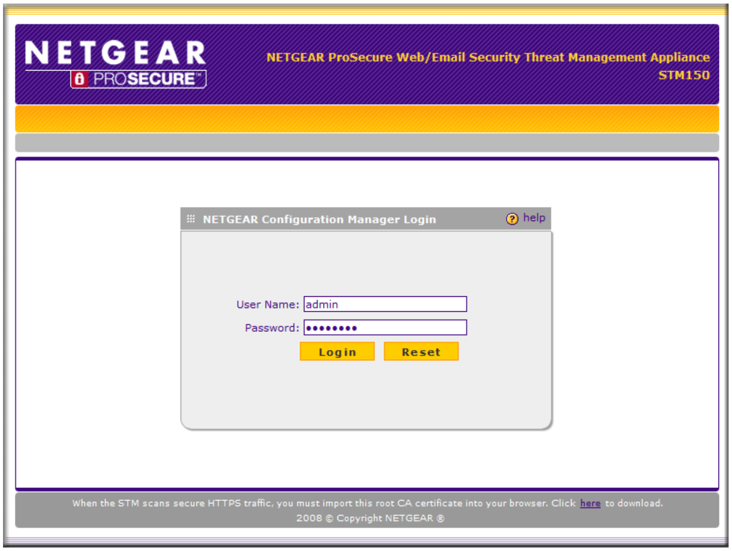


https://192.168.1.201

Figure 2-4

Note: The STM150 factory default IP address is 192.168.1.201. If you changed it, you must use the IP address you assigned it.

2. When prompted, enter **admin** for the User Name and **password** for the Password.



NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance
STM150
NETGEAR Configuration Manager Login
help
Login
Reset

User Name: admin

Password: ••••••••

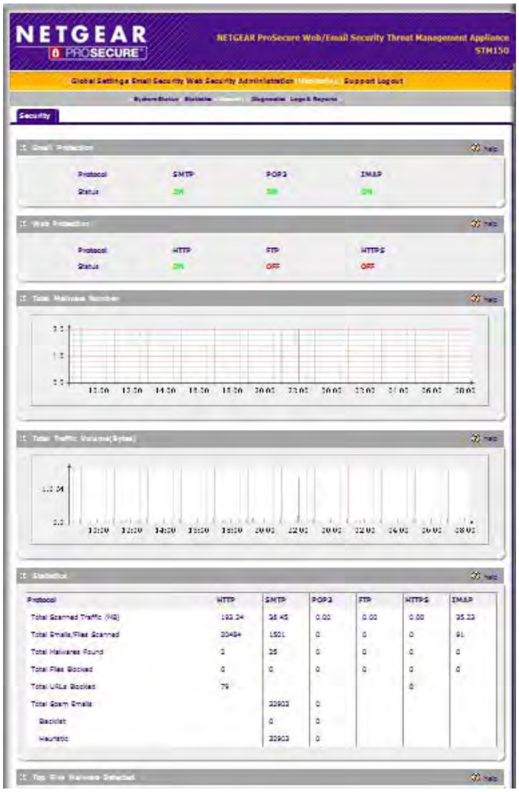
When the STM scans secure HTTPS traffic, you must import this root CA certificate into your browser. Click here to download.

2008 © Copyright NETGEAR ®

Figure 2-5

Note: When the STM scans secure HTTPS traffic, import its root CA certificate into your browser. Click the link at the bottom of the login screen to download it.

3. Click **Login.** The default Monitoring > Security page displays.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
Global Settings Email Security Web Security Administration Monitoring Support Logout
System Status Statistics Security Diagnostics Logs & Reports
Security
Email Protection
Web Protection
Total Malwares Number
Total Traffic Volume(Bytes)
Statistics
Top Five Malware Detected
help

Protocol	SMTP	POP3	IMAP
Status	ON	ON	ON

Protocol	HTTP	FTP	HTTPS
Status	ON	OFF	OFF

Protocol	HTTP	SMTP	POP3	FTP	HTTPS	IMAP
Total Scanned Traffic (MB)	193.24	26.45	0.00	0.00	0.00	25.23
Total Emails/Files Scanned	20494	1501	0	0	0	91
Total Malwares Found	2	25	0	0	0	0
Total Files Blocked	0	0	0	0	0	0
Total URLs Blocked	79				0	
Total Spam Emails		22903	0			
Blacklist		0	0			
Heuristic		22903	0			

Figure 2-6

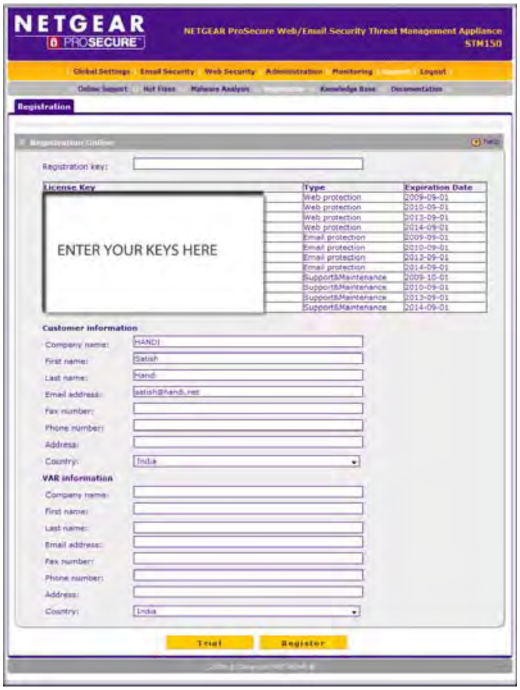
Note: During the initial setup, the setup wizard displays when your first log in; afterward the login takes you to the system status page.

The Support tab on the main menu contains links to the online NETGEAR STM150 product documentation and support knowledgebase.

Note: After 10 minutes of inactivity (the default login time-out), you are automatically logged out.

Registering the STM150

To receive threat management component updates and technical support, you need to register your STM150 appliance.



Registration key:

License Key	Type	Expiration Date
ENTER YOUR KEYS HERE	Web protection	2009-09-01
	Web protection	2010-09-01
	Web protection	2013-09-01
	Web protection	2014-09-01
	Email protection	2009-09-01
	Email protection	2010-09-01
	Email protection	2013-09-01
	Email protection	2014-09-01
	Support&Maintenance	2009-10-01
	Support&Maintenance	2010-09-01
	Support&Maintenance	2013-09-01
	Support&Maintenance	2014-09-01

Customer information

Company name: HANDI
First name: Satish
Last name: Handi
Email address: satish@handi.net
Fax number:
Phone number:
Address:
Country: India

VAR information

Company name:
First name:
Last name:
Email address:
Fax number:
Phone number:
Address:
Country: India

Figure 2-7

The registration key (see “Service Registration Card with License Key(s)” on page 1-4) is provided in the product package.

If your STM150 is connected to the Internet, you can register it online.

1. Select **Support** > **Registration**. The registration page displays
2. Enter the registration key and contact information.
3. Click **Register**.
4. Repeat steps 2 and 3 for each key.

Use the Setup Wizard to Complete the Configuration

Follow the wizard prompts to configure these settings:

- Network settings - If these were set earlier, skip this page or update these as needed.
- Set the system time (NTP server) and time zone.
- Configure Email Security settings.
- Configure Web Security.
- Specify the Email notification server to receive logs, alerts, and reports.
- Configure update settings.
- Configure Web category blocking.

Follow the guidelines below for completing the Setup Wizard.

Setup Wizard Options

For most settings, the default scan options will be the appropriate choices. Also, update the basic network settings only if you did not follow the instructions in the Installation Guide.

Email Security

On this wizard page, enable the network services you want to scan and specify the ports for each, select the scan actions, set the scan exceptions, and configure the maximum file size to scan.

Note: Setting the maximum file size to a high value may affect the STM150's performance. The default value is recommended, which is sufficient to detect the vast majority of threats.

Tip: To enhance performance, you may disable scanning of any protocols that will be seldom or never used. Be mindful of the difference between user and server generated traffic. For example, your mail server may not use IMAP but some users may configure IMAP clients.

Web Security

On this wizard page, enable the network services you want to scan and specify the ports for each, select the scan actions, set the scan exceptions, and configure the maximum file size to scan. Check the Streaming checkbox for an even more transparent user Web browsing experience.

Email Notification Server

On this wizard page, type the email address that you want to appear in the notification email as sender. For example, you can type '`STM150@mydomain.com`'. Enter the SMTP server host name or IP address. The STM150 will send notification emails via this SMTP server. If the SMTP server requires authentication, select the **This server requires authentication** check box, and then enter the user name and password.

Note: A different SMTP port number can be configured under the email notification server settings.

Update Settings

The STM150 has four main components, which include a pattern file, the scan engine, operating system (OS), and software. To ensure up-to-date protection against malware, perform updates regularly. The default update frequency is set to hourly, since updates to the pattern file are released on an *hourly basis*.

If the computers on the network connect to the Internet through an HTTPS proxy server, enter the IP address and port number of the proxy server. If a firewall is installed on the local network, make sure that Internet access is allowed via port 443. If the proxy server requires authentication, enter a user name and password.

Web Categories

The STM150 lets you choose from a list of Web content categories you can block from being accessed from your network. Check those you wish to block.

Apply the Changes

To confirm and apply the STM150 settings that you have configured, click **Apply**. The STM150 will reboot to apply the updated settings.

Verifying the STM150 Installation

Test the STM150 before deploying it in a live production environment. The following instructions walk you through a couple of quick tests designed to ensure that your STM150 is functioning correctly.

Testing Connectivity

Do the following to verify that network traffic can pass through the STM150:

- Ping an Internet URL.
- Ping the IP address of a device on either side of the STM150.

Testing HTTP Scanning

If client computers have direct access to the Internet through your LAN, try to download the eicar.com test file from

http://www.eicar.org/download/eicar.com

The `eicar.com` test file is a legitimate DOS program and is safe to use because it is not a malware and does not include any fragments of malware code. The test file is provided by EICAR, an organization which unites efforts against computer crime, fraud, and misuse of computers or networks.

1. Log on to the STM150 interface, and then verify that HTTP scanning is enabled. For instructions, see "Customizing Email Scanning Settings" on page 4-2 and "Customizing Web Scanning Settings" on page 4-12.
2. Check the downloaded file and note the attached malware information file.

What to Do Next

You have completed setting up and deploying the STM150 to the network. The STM150 is now set up to scan the protocols/services you specified for malware and perform updates based on the configured update source and frequency.

If you need to change the settings or to view reports or logs, connect to the STM150 Web interface (using the IP address you assigned to the STM150 during the preconfiguration process), and then log on.

Refer to the succeeding chapters for information on performing additional tasks using the Web interface.

Chapter 3
Performing System Management Tasks

This chapter provides information on other tasks that you can perform after setting up and configuring the STM150.

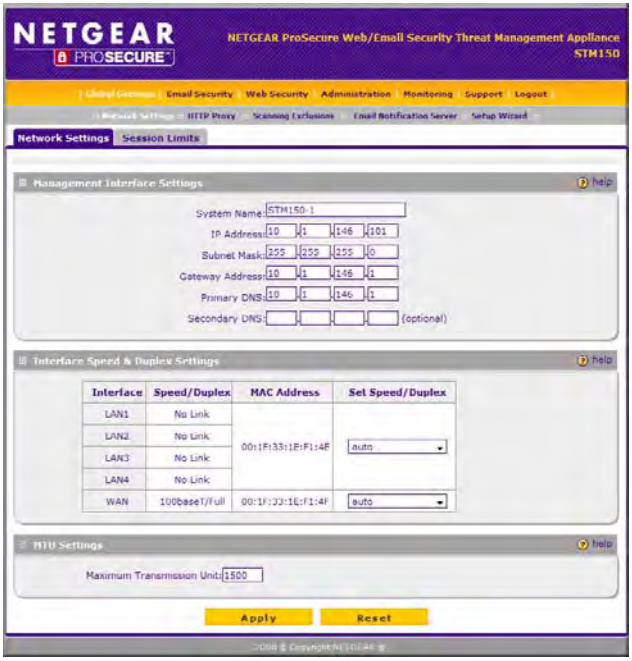
This chapter contains the following sections:

Modifying System Settings

This section covers modifying the settings you initially set in the Setup Wizard, or making other system settings changes.

Configuring Network Settings

A valid IP address is required for the STM150 to retrieve online updates. It is also needed for access to the STM150 management web GUI. Go to Global Settings > Network Setting to enter the system name and other network settings.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance
STM150
Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout
Network Settings | HTTP Proxy | Scanning Exclusions | Email Notification Server | Setup Wizard
Network Settings
Session Limits
help
Apply
Reset
2008 © Copyright NETGEAR ®

Management Interface Settings

System Name: STM150-1

IP Address: 10 . 1 . 146 . 101

Subnet Mask: 255 . 255 . 255 . 0

Gateway Address: 10 . 1 . 146 . 1

Primary DNS: 10 . 1 . 146 . 1

Secondary DNS: (optional)

Interface Speed & Duplex Settings

Interface	Speed/Duplex	MAC Address	Set Speed/Duplex
LAN1	No Link	00:1F:33:1E:F1:4E	auto
LAN2	No Link		
LAN3	No Link		
LAN4	No Link		
WAN	100baseT/Full	00:1F:33:1E:F1:4F	auto

MTU Settings

Maximum Transmission Unit: 1500

Figure 3-1

For other devices connected to the STM150 (such as a firewall or a switch), you now have an option to manually change the duplex settings. This feature will allow STM150 to integrate with other devices seamlessly. The default setting is Auto.

For example, if the firewall is connected to LAN-1 on the STM150 with the 10M/s connection setting, you may go to the STM150 Web interface and make the changes. Go to Global Settings > Network Setting. Under Speed, change the duplex setting for LAN-1.

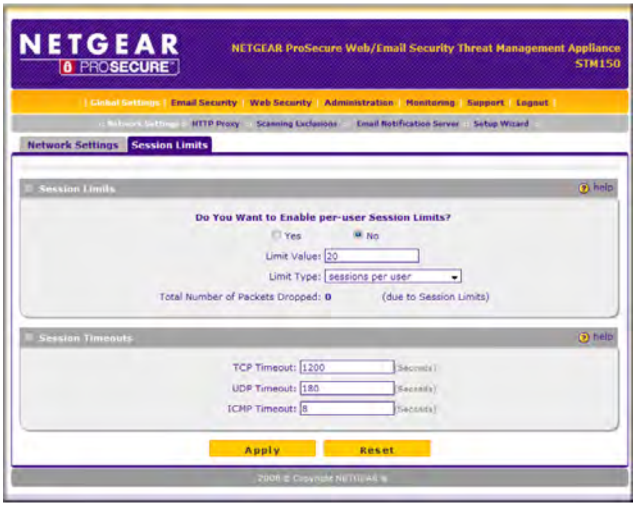
The maximum transmission unit (MTU) is the largest physical packet size that a network can transmit. Packets that are larger than the MTU value will be divided into smaller packets before they are sent, an action that will prolong the transmission process.

Most networks have an MTU value of 1500. To minimize transmission delays, assure that the MTU setting of the STM150 matches your network.

Clicking on Reset on the Global Settings > Network Setting screen will reset all settings back to their default values (IP 192.168.1.201, MTU 1500...etc).

Enabling Session Limits and Timeouts

You enable session limits and timeouts on the Global Settings > Network Setting > Session Limit screen.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout
Network Settings | HTTP Proxy | Scanning Exclusions | Email Notification Server | Setup Wizard
Network Settings
Session Limits
help
help
Apply
Reset
2008 © Copyright NETGEAR ®

Session Limits

Do You Want to Enable per-user Session Limits?

○ Yes ● No

Limit Value: 20

Limit Type: sessions per user

Total Number of Packets Dropped: 0 (due to Session Limits)

Session Timeouts

TCP Timeout: 1200 (Seconds)

UDP Timeout: 180 (Seconds)

ICMP Timeout: 8 (Seconds)

Figure 3-2

This page allows you to specify total number sessions per user (IP) allowed across the router. Session limiting is disabled by default. When session limiting is enabled, the STM150 will set the maximum number of sessions per IP either as a percentage of the maximum sessions or as an absolute number of maximum sessions.

To increase the maximum number of sessions per IP, check Yes under Do you want to enable Session Limit? The Percentage of Max Sessions option is computed on the total connection capacity of the device. The Number of Sessions option specifies the maximum number of sessions that should be allowed via the STM150 from a single source machine. Please note that some protocols like ftp, rstp create 2 sessions per connection which should be considered when configuring session limiting. Enter the new session limit under User Limit.

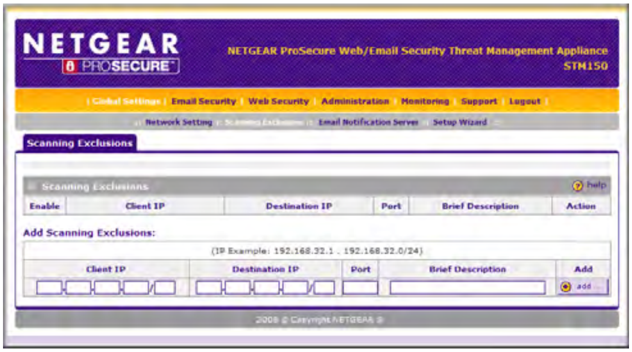
The Session Timeout section allows you to manually define the TCP, UDP, and ICMP timeout values. If a session goes without data flow longer than the configured values, the session will be terminated by the system. The default session timeout of TCP, UDP and ICMP is 1200, 800 and 8 seconds. Enter the timeout values in their respective fields.

Scanning Exclusions

To enhance system performance, you may add trusted hosts or connections to this list. The STM150 will no longer scan these connections based on the specified hosts or ports.

To enter a scanning exclusion rule

1. On the menu, click **Global Settings** > **Scanning Exclusions**.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance
STM150
Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout
Network Setting | Scanning Exclusions | Email Notification Server | Setup Wizard
Scanning Exclusions
Scanning Exclusions
help
add
2008 © Copyright NETGEAR ®

Enable	Client IP	Destination IP	Port	Brief Description	Action

Add Scanning Exclusions:

(IP Example: 192.168.32.1 . 192.168.32.0/24)

Client IP	Destination IP	Port	Brief Description	Add
. . . /	. . . /			● add

Figure 3-3

2. Enter the IP address (range) in their respective fields. Either the Client IP or the Destination IP can be left blank depending on what traffic you are excluding.
3. Enter the destination port number in the Port field.
4. Enter a brief description of the rule in the Brief Description field.
5. Click **Add**.

   The rule will now appear in the list and be enabled. Check the Enable box to enable/disable the rule.

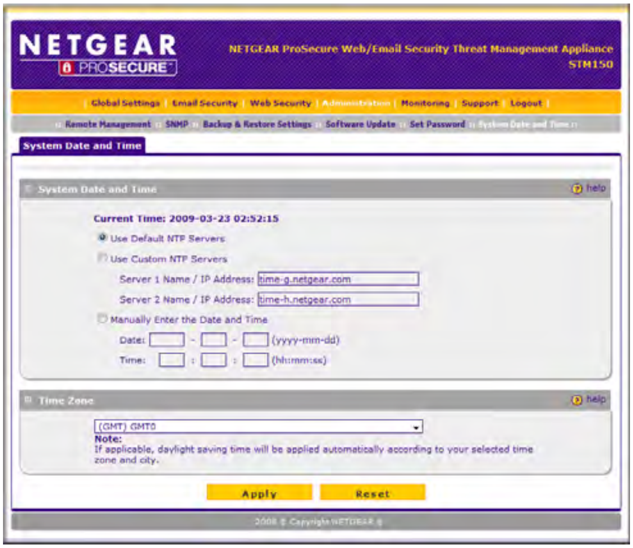
To delete a scanning exclusion rule: click **Delete** next to the rule you wish to delete.

Setting the System Time

Setting the correct system time and time zone ensures that the date and time recorded in the STM150 logs are accurate. Changing the time zone requires a reboot to apply the updated settings.

To set the system time

1. On the menu, click **Administration** > **Time Zone**.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout
Remote Management | SNMP | Backup & Restore Settings | Software Update | Set Password | System Date and Time
System Date and Time
help
Apply
Reset
2008 © Copyright NETGEAR ®

System Date and Time

Current Time: 2009-03-23 02:52:15

● Use Default NTP Servers

○ Use Custom NTP Servers

Server 1 Name / IP Address: time-g.netgear.com

Server 2 Name / IP Address: time-h.netgear.com

○ Manually Enter the Date and Time

Date: __ - __ - __ (yyyy-mm-dd)

Time: __ : __ : __ (hh:mm:ss)

Time Zone

(GMT) GMT0

Note:
If applicable, daylight saving time will be applied automatically according to your selected time zone and city.

Figure 3-4

2. You can use either the default NTP server or a custom NTP server. Set the system time either by:
   - Using a Network Time Protocol (NTP) server. A list of public NTP servers is available at `http://ntp.isc.org/bin/view/Servers/WebHome`.
   - Manually entering the date and time
3. In **Time Zone**, select the correct time zone.
4. Click **Apply**. If the time zone has changed, a reboot confirmation will appear.

Specifying the Notification Server

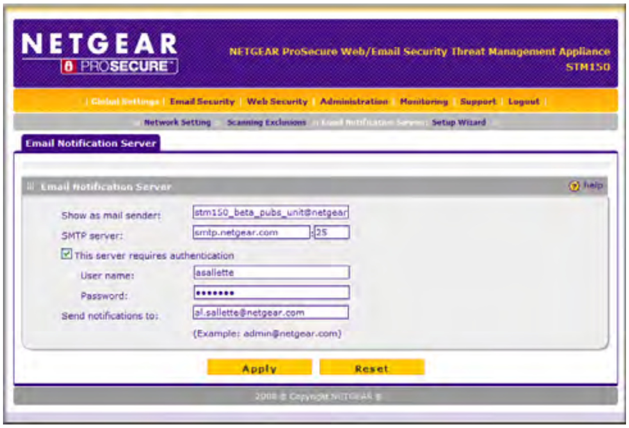
For the STM150 to send out alerts, reports, and logs via email, an SMTP server must be specified on the Global Settings > Email Notification Server page.

> **Note:** If you do not set a notification server, the STM150 will be unable to send email alerts to you.

Note that same SMTP server will also send you logs and reports. If you do not specify an SMTP server, the STM150 will still generate reports and logs, but it will be unable to send them to you or other members of your organization via email.

To specify a notification server

1. On the menu, go to **Global Settings > Email Notification Server**.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout
Network Setting | Scanning Exclusions | Email Notification Server | Setup Wizard
Email Notification Server
help
Apply
Reset
2008 © Copyright NETGEAR ®

Email Notification Server

Show as mail sender: stm150_beta_pubs_unit@netgear

SMTP server: smtp.netgear.com : 25

☑ This server requires authentication

User name: asallette

Password: •••••••

Send notifications to: al.sallette@netgear.com

(Example: admin@netgear.com)

Figure 3-5

2. In **Show as mail sender**, type an email address that will appear in the **From** field when the email is received by recipients. For example, you can type `‘STM150@mydomain.com’`.
3. In **SMTP server**, type the host name or IP address of the SMTP server on the network that you want to use.
4. If the SMTP server you specified above requires a user name and password to send mail messages, select the **This server requires authentication** check box, and then type a valid user name and password in the corresponding text boxes.

5. In **Send notification to**, type up to the email addresses to which you want to send alerts (for example, `admin@company.com`). You can send alerts to up to 3 recipients; separate each email address with a comma.
6. Click **Save Changes**.

Customizing Email Alerts

After you set an SMTP server to use for notification, you need to specify the types of alerts that you want the STM150 to send out. The STM150 provides four types of alerts – update failed alert, license expiration alert, malware alert, and outbreak alert.

If the update failed alert is enabled, the STM150 will send an email notification to the administrator in the event of an update failure.

If the license expiration alert is enabled, the STM150 will send an email notification to the administrator when a license expires.

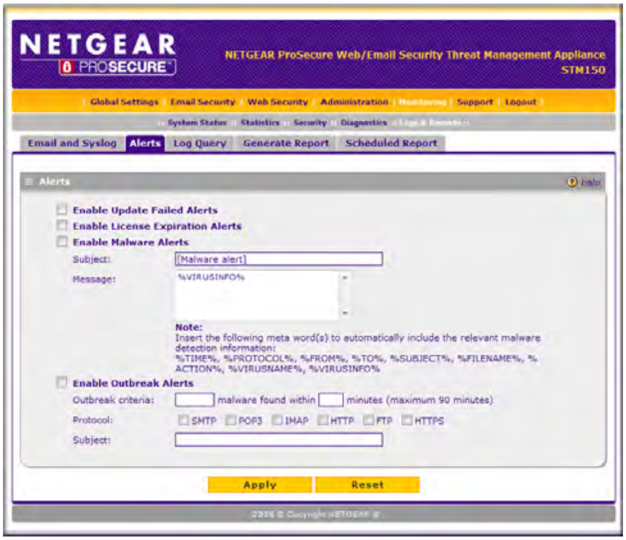
Note: License expiration email notification is sent 45 days prior to expiration, and by the second day of expiration. For trial licenses, the notification also is sent 15 days before expiration.

If malware alert is enabled, the STM150 will send email alerts for each malware that is detected on the network. Alerts for malware incidents can be customized using meta tags to specify the information to include in the alert. Alert information can include malware name, protocol used, date and time detected, etc.

If outbreak alert is enabled, the STM150 will send email alerts when a certain number of malware is detected on the network within a specified period. Outbreak alerts can be enabled for all protocols scanned and you can manually set the outbreak criteria.

To enable system administrator email alerts

1. On the menu, go to **Monitoring** > **Logs & Reports** > **Alerts**.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout
System Status | Statistics | Security | Diagnostics | Logs & Reports
Email and Syslog | Alerts | Log Query | Generate Report | Scheduled Report
help
Apply
Reset
2006 © Copyright NETGEAR ®

Alerts

□ Enable Update Failed Alerts

□ Enable License Expiration Alerts

□ Enable Malware Alerts

Subject: [Malware alert]

Message: %VIRUSINFO%

Note:
Insert the following meta word(s) to automatically include the relevant malware detection information:
%TIME%, %PROTOCOL%, %FROM%, %TO%, %SUBJECT%, %FILENAME%, %ACTION%, %VIRUSNAME%, %VIRUSINFO%

□ Enable Outbreak Alerts

Outbreak criteria: ____ malware found within ____ minutes (maximum 90 minutes)

Protocol: □ SMTP □ POP3 □ IMAP □ HTTP □ FTP □ HTTPS

Subject: ____

Figure 3-6

2. Configure the **Enable Update Failed Alerts, Enable License Expiration Alerts, Enable Malware Alerts, or Enable Outbreak Alerts** check boxes as you prefer.
   - For Malware Alerts, in **Message**, use the meta tags to specify the information that will be included in the alert message. The default message includes the `%VIRUSINFO%` tag, which dynamically inserts information on the malware that has been detected. In **Subject**, accept the default alert subject or create your own.
   - In Outbreak Alerts, configure **Outbreak Criteria** to define what constitutes the outbreak criteria by specifying the number of malware that must be detected during a specified period of time (in minutes). In **Subject**, type the email subject that you want to appear in the outbreak alert.
   - In **Protocols**, select the check boxes for the protocols/services for which you want to enable the outbreak alert.
3. Click **Apply**.

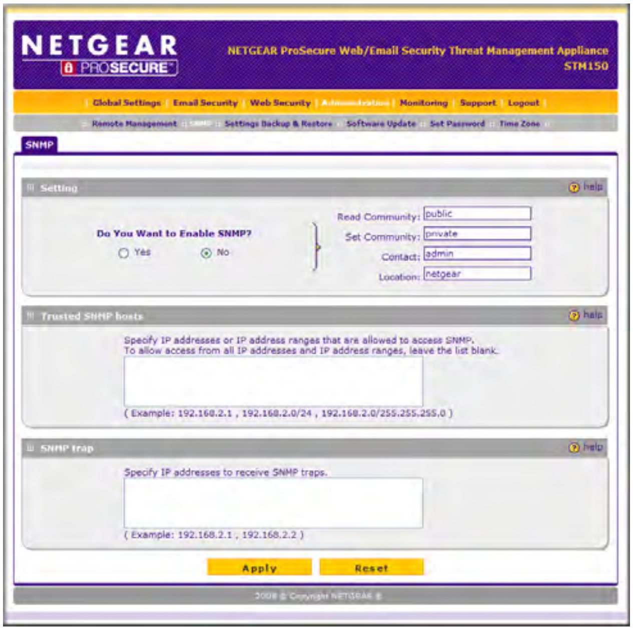
Configuring SNMP Settings

Simple Network Management Protocol (SNMP) is an application layer (Layer 7) protocol that is used by network management systems for monitoring the status of network-connected devices. SNMP enables administrators to monitor network performance, identify bottlenecks and plan for network expansion.

The STM150 provides support for report aggregation via SNMP version 1. You can configure it to send SNMP traps to management stations on the network.

To configure the SNMP settings

1. On the menu, click **Administration** > **SNMP**.



Setting

Do You Want to Enable SNMP?

○ Yes ● No

Read Community: public

Set Community: private

Contact: admin

Location: netgear

Trusted SNMP hosts

Specify IP addresses or IP address ranges that are allowed to access SNMP.
To allow access from all IP addresses and IP address ranges, leave the list blank.

(Example: 192.168.2.1 , 192.168.2.0/24 , 192.168.2.0/255.255.255.0)

SNMP trap

Specify IP addresses to receive SNMP traps.

(Example: 192.168.2.1 , 192.168.2.2)

Figure 3-7

2. Select the **Enable SNMP Yes** radio button.

- In **Read community**, type the community name that SNMP management stations on the network need to use to retrieve the STM150’s SNMP parameters.
- In **Set community** (write), type the community name that management stations need to use to set or write the STM150’s SNMP parameters.

- In **Contact** (optional), type the name of the person or department responsible for managing the STM150 appliance.
- In **Location** (optional), type the physical location of the STM150 appliance.

3. In **Trusted SNMP hosts**, type the IP addresses of the computers to which you want to grant GET and SET privileges on the STM150. Only the computers with IP addresses listed here will be able to enable/disable services, reboot the STM150, and reset accumulated its statistics.
4. In **SNMP trap**, type the IP addresses of the SNMP management stations to which you want SNMP traps to be sent.
5. Click **Apply**.

Supported MIB Browsers

After you configure the SNMP settings, the only other thing that you need to do is add the IP address of the STM150 into the management information base (MIB) browsers on which you want to receive the SNMP notifications. Refer to documentation of your MIB browser for instructions.

The following are recommended MIB browsers for receiving the STM150 SNMP notifications:

- MG-Soft
- SNMP
- Net-SNMP (Linux Text)
- SNMP Browser for KDE

The STM150 MIB structure is automatically downloaded by management stations. You should start receiving notifications after you enable SNMP on the STM150 and add the its IP address into your MIB browsers.

Defining Trusted SNMP Hosts

In Trusted SNMP hosts, type the IP addresses of the computers to which you want to grant GET and SET privileges on the STM150. Only the computers with IP addresses listed here will be able to access the SNMP features of STM150.

To define SNMP Traps

In SNMP trap, type the IP addresses of the SNMP management stations to which you want SNMP traps to be sent.

Backing Up and Restoring Configurations

The STM150 provides backup and restore features to ensure speedy recovery from system errors or configuration on an additional STM150 appliance with the same language and management software versions. Access the backup and restore functions at Administration > Settings Backup & Restore.

The backup feature saves all the STM150 settings to a file. These settings include:

- Network settings – IP address, subnet mask, gateway, etc.
- Scan settings – Services to scan, primary and secondary actions, etc.
- Update settings – Update source, frequency, etc.
- Anti-spam settings – Whitelist, blacklist, content filtering settings, etc.

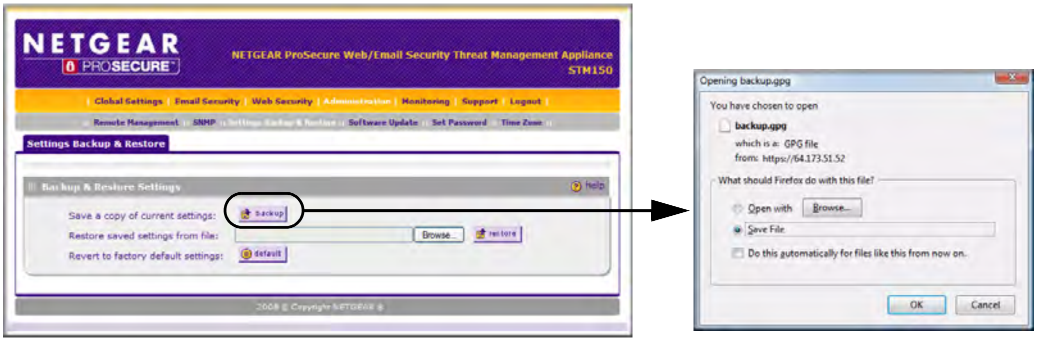
> **Tip:** You can use a backup file to export all settings to another STM150 appliance that has the same language and management software versions. Remember to change the IP address of the second STM150 appliance before deploying it to eliminate IP address conflicts on the network.

Backing Up the STM150 Configuration

Back up your STM150 settings periodically and store the backup file in a safe place.

To Back Up the STM150 Settings

1. On the menu, click **Administration** > **Settings Backup & Restore**. The Backup and Restore page appears.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
| Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout |
Remote Management | SNMP | Settings Backup & Restore | Software Update | Set Password | Time Zone
Settings Backup & Restore
Backup & Restore Settings
help
backup
Browse...
restore
default
2008 © Copyright NETGEAR ®
Opening backup.gpg
Browse...
OK
Cancel

Save a copy of current settings:

Restore saved settings from file:

Revert to factory default settings:

You have chosen to open

backup.gpg

which is a: GPG file

from: https://64.173.51.52

What should Firefox do with this file?

○ Open with

● Save File

□ Do this automatically for files like this from now on.

Figure 3-8

2. For the Save a copy of current settings option, click **Backup**. A dialog box appears, showing the file name of the backup file (`backup.gpg`).
3. Click **Save file**, and then click **OK**.
4. Open the folder where you saved the backup file, and then verify that it has been saved successfully.

Restoring A Configuration

Use the restore feature to import the STM150 settings that you previously backed up.

⚠	**Warning:** Only restore settings that were backed up from the same software version. Restoring settings from a different software version can corrupt your backup file or the STM150 system software.

To restore the STM150 settings

1. Copy the backup file to the admin computer.
2. For the Restore saved settings from file option, click **Browse**, and then locate the backup file.
3. Click **Restore**.

Resetting to Factory Defaults

Warning: If you reset the unit, all configuration settings will be lost, the default password will be restored, and you will need to re-register the product license.

You can use the default button on the Backup & Restore Settings page to revert to factory default settings, or you can use the reset button on the back of the unit.

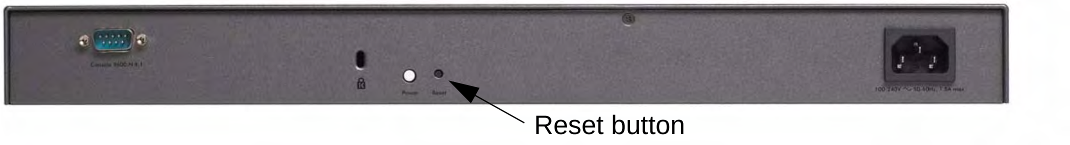


Figure 3-9

Use the Reset button to restore the factory defaults. Use a sharp object, press and hold this button for about ten seconds until the front panel Test light flashes to reset the unit to factory default settings.

Restarting the STM150

Restarting the STM150 will temporarily terminate all network connections that pass through it. Network connection is restored as soon as the restart and startup processes are completed, usually within a minute or two.

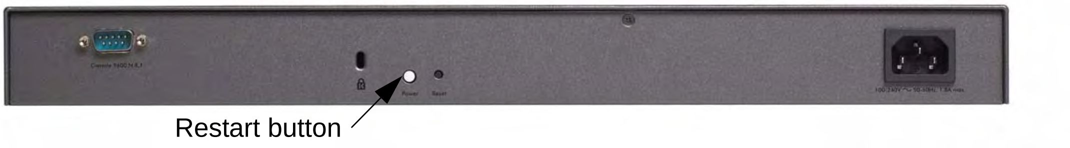
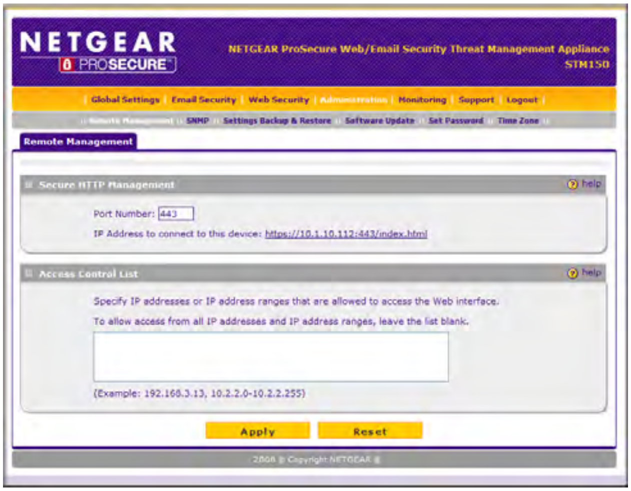


Figure 3-10 New Photo

On the rear panel, press the Restart button: this restarts the unit; it does not reset the appliance to its factory defaults.

Enabling Remote Management

To enable remote management, go to **Administration** > **Remote Management**.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout
Remote Management | SNMP | Settings Backup & Restore | Software Update | Set Password | Time Zone
Remote Management
help
help
Apply
Reset
2008 © Copyright NETGEAR ®

Secure HTTP Management

Port Number: 443

IP Address to connect to this device: https://10.1.10.112:443/index.html

Access Control List

Specify IP addresses or IP address ranges that are allowed to access the Web interface.

To allow access from all IP addresses and IP address ranges, leave the list blank.

(Example: 192.168.3.13, 10.2.2.0-10.2.2.255)

Figure 3-11

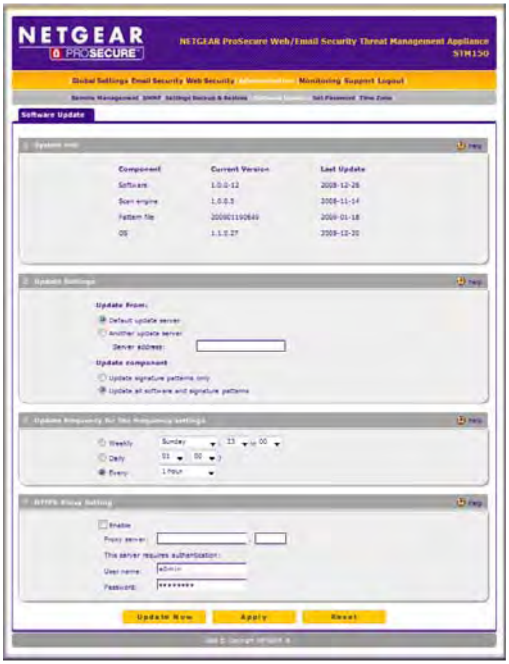
Enter the port number you wish to use. You may enter port 443 or a port ranging from 1024 to 65535. Some ports which could have been used by the system (such as: 2080, 8081...) cannot be used here. Click **Apply**.

Click Reset to reset the port to the default value (443).

You can also specify IP addresses or IP address ranges that you want to allow access to the Web interface.

Administering Software Updates

The STM150 has four main components – pattern file, scan engine, OS, and software. To ensure up-to-date protection against malware, perform updates regularly.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
Global Settings Email Security Web Security Administration Monitoring Support Logout
Remote Management SNMP Settings Backup & Restore Software Update Set Password Time Zone
Software Update
Help
Update Now
Apply
Reset

System Info

Component	Current Version	Last Update
Software	1.0.0-12	2008-12-26
Scan engine	1.0.0.3	2008-11-14
Pattern file	200901190649	2009-01-18
OS	1.1.0.27	2008-12-30

Update Settings

Update From:

● Default update server

○ Another update server

Server address:

Update component

○ Update signature patterns only

● Update all software and signature patterns

Update Frequency

○ Weekly Sunday 13 to 00

○ Daily 01 00

● Every 1 hour

HTTPS Proxy Setting

□ Enable

Proxy server:

This server requires authentication:

User name: admin

Password: ********

Figure 3-12

The STM150 provides two methods of updating its components:

- Scheduled (automatic) update
- Manual update

Configuring Scheduled Updates

Enabling scheduled updates ensures that your the STM150 automatically gets the latest components from the NETGEAR update server.

To configure scheduled updates

1. On the menu, go to **Administration > Software Update**.
2. In **Update From**, select an update source. The default update source is the NETGEAR update server.

   If NETGEAR or its authorized reseller provided you with an alternative update source, or if you have set up an update source on the intranet, you can also specify this source by selecting **Connect to another update server**, and then entering the IP address or host name of the alternative update source.
3. If you want the STM150 to check for and update the pattern file only, select the **Update signature patterns to** check box. If you want the STM150 to update all components (including the pattern file), leave the box unchecked.
4. In **Update Frequency**, specify how often you want the STM150 to check for and download updates from the update source. You can choose Weekly, Daily, or Hourly.
5. If computers on the network connect to the Internet via a proxy server, select the **Use HTTPS Proxy Server** check box, and then enter the proxy server information and, if applicable, a user name and password.

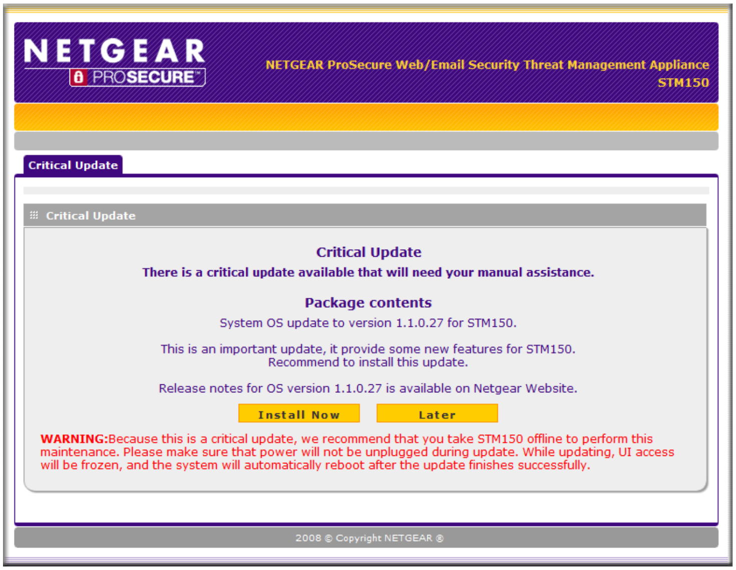
   If a firewall is installed on the local network, make sure port 443 is allowed access to the Internet.
6. Click **Save Changes**.

Performing a Manual Update

If you want to immediately check for and download available updates, you can perform a manual update. On the menu, click **Update Now** near the bottom of the page.

Applying a Software Update that Requires a Reboot

If a downloaded update requires a reboot, you will be prompted to perform the update upon login to the system.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
Critical Update
Critical Update

Critical Update

There is a critical update available that will need your manual assistance.

Package contents

System OS update to version 1.1.0.27 for STM150.

This is an important update, it provide some new features for STM150.
Recommend to install this update.

Release notes for OS version 1.1.0.27 is available on Netgear Website.

WARNING:Because this is a critical update, we recommend that you take STM150 offline to perform this maintenance. Please make sure that power will not be unplugged during update. While updating, UI access will be frozen, and the system will automatically reboot after the update finishes successfully.

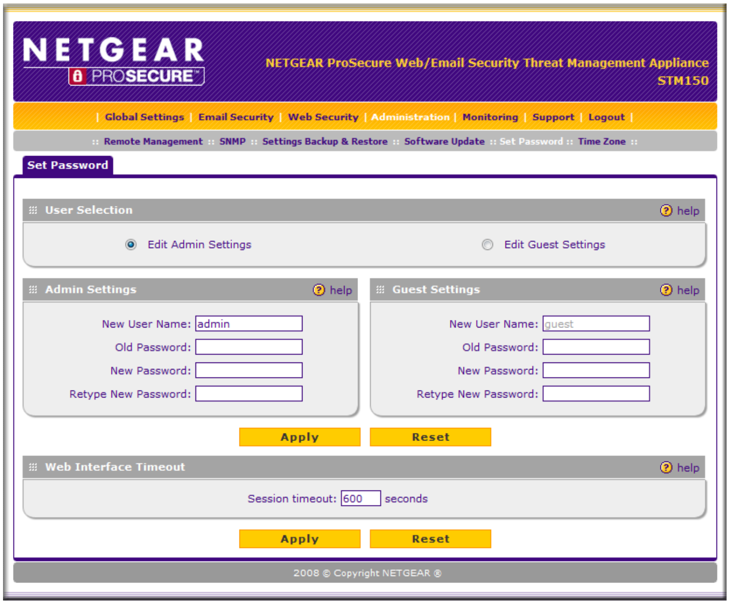
2008 © Copyright NETGEAR ®

Figure 3-13

The update notice will provide information about the update, allow you to install it now or install it later, and warn you if the update will reboot the system.

Administering Admin Login Timeouts and Passwords

The STM150 specifies one Administrator account (Admin) and one guest account. You can use this section to change the user name or password for either account, and adjust the admin login time setting.


NETGEAR PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
| Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Restore :: Software Update :: Set Password :: Time Zone ::
Set Password
help
Apply
Reset
Apply
Reset

User Selection

● Edit Admin Settings ○ Edit Guest Settings

Admin Settings

New User Name: admin
Old Password:
New Password:
Retype New Password:

Guest Settings

New User Name: guest
Old Password:
New Password:
Retype New Password:

Web Interface Timeout

Session timeout: 600 seconds

2008 © Copyright NETGEAR ®

Figure 3-14

To edit the Admin User Name, from the main menu, click **Administration** > **Set Password**.

1. Select Edit Admin Settings
2. Under Admin Settings, type the new user name under the New User Name field.
3. Enter the current password under the Old Password field.
4. Click **Apply**.

To edit the Admin Password, from the main menu, click **Administration** > **Set Password**.

1. Select Edit Admin Settings
2. Enter the current password (password is the factory default) under the Old Password field.

3. Enter the new password under the New Password field.
4. To confirm, enter the new password again under the Retype New Password field.
5. Click **Apply**.

To edit the Guest User Name, from the main menu, click **Administration > Set Password**.

1. Select Edit Guest Settings
2. Under Guest Settings, type the new user name under the New User Name field.
3. Enter the current password (guest is the factory default) under the Old Password field.
4. Click **Apply**.

To edit the Guest Password, from the main menu, click **Administration > Set Password**.

1. Select Edit Guest Settings
2. Enter the current password under the Old Password field.
3. Enter the new password under the New Password field.
4. To confirm, enter the new password again under the Retype New Password field.
5. Click **Apply**.

You can configure STM150 to automatically log off any of its Web interface sessions if no activity is detected within a specified period of time. To configure Web interface timeout, from the main menu, click **Administration > Set Password**.

In Session Timeout under Web Interface Timeout, specify the number seconds of inactivity (timeout) after which the Web interface session will be terminated. The default timeout is 600 seconds. Click **Apply** to save your changes.

Chapter 4
Customizing Scans

This chapter provides information on how to optimize the ProSecure Web/Email Security Threat Management Appliance STM150 scan settings.

Topics discussed include:

- "Default Scan Settings" on page 4-1
- "Customizing Email Scanning Settings" on page 4-2
- "Customizing Web Scanning Settings" on page 4-12
- "Configuring FTP Scan" on page 4-25

Default Scan Settings

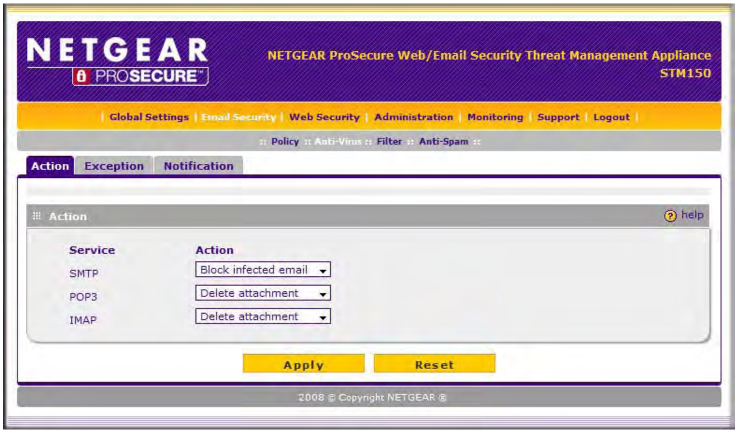
Table 1 lists the default scan and update settings, which work in most settings.

Table 1 STM150 Default Settings

	Default Setting		
Scan Type	**Enabled**	**Disabled**	**Default Actions**
HTTP	X		Delete file
POP3	X		Delete attachment
SMTP	X		Block infected email
FTP	X		Delete file
HTTPS		X	
IMAP	X		Delete attachment
Update	X		Check every hour for updated components

Customizing Email Scanning Settings

The Email Security pages allow you to enable and disable scanning of supported network services (protocols), set the scan actions, and configure the maximum file size to scan.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout
:: Policy :: Anti-Virus :: Filter :: Anti-Spam ::
Action
Exception
Notification
Action
help
Apply
Reset
2008 © Copyright NETGEAR ®

Service	Action
SMTP	Block infected email
POP3	Delete attachment
IMAP	Delete attachment

Figure 4-1

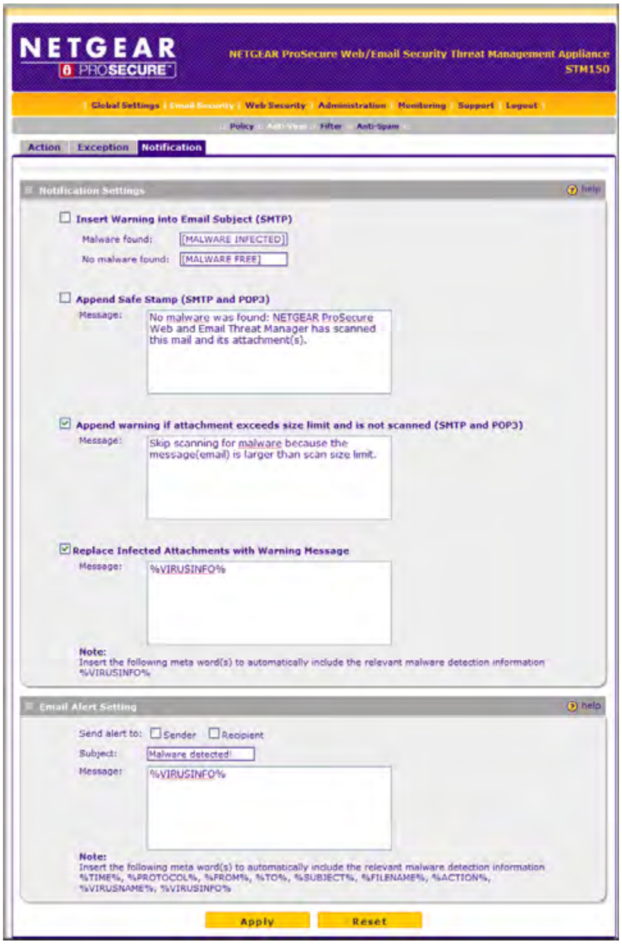
In the Email Security > Anti-Virus > Action page, set an action that you want the STM150 to perform when it detects a threat. The STM150 can block and delete infected emails or attachments. Simply select the action you wish to take from the drop down menu. Before configuring the scan options for your network services, make sure you enable scanning of the particular service.

In the Email Security > Anti-Virus > Exception page, set the maximum file size that the STM150 will scan. The STM150 can scan files up to 25,600KB (25MB) in size.

Note: Setting the maximum file size to a high value may affect the performance of STM150. NETGEAR recommends keeping this value set to the default 8,192 KB).

End User Email Notification Settings

To configure the notification options for email scan, go to
Email Security > **Anti-Virus > Notification Settings** on the menu.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout
Policy | Anti-Virus | Filter | Anti-Spam
Action | Exception | Notification
Notification Settings
help

□ Insert Warning into Email Subject (SMTP)

Malware found: [MALWARE INFECTED]

No malware found: [MALWARE FREE]

□ Append Safe Stamp (SMTP and POP3)

Message: No malware was found: NETGEAR ProSecure Web and Email Threat Manager has scanned this mail and its attachment(s).

☑ Append warning if attachment exceeds size limit and is not scanned (SMTP and POP3)

Message: Skip scanning for malware because the message(email) is larger than scan size limit.

☑ Replace Infected Attachments with Warning Message

Message: %VIRUSINFO%

Note:
Insert the following meta word(s) to automatically include the relevant malware detection information
%VIRUSINFO%

Send alert to: □ Sender □ Recipient

Subject: Malware detected!

Message: %VIRUSINFO%

Note:
Insert the following meta word(s) to automatically include the relevant malware detection information
%TIME%, %PROTOCOL%, %FROM%, %TO%, %SUBJECT%, %FILENAME%, %ACTION%, %VIRUSNAME%, %VIRUSINFO%

Figure 4-2

The following options are available on the Notification Settings page.

Insert Warning into Email Subject Line (SMTP)

You may insert a tag at the beginning of the email subject line as notification. The tag is customizable, for example, `[Malware Infected]`.

Select the I**nsert Warning into Email Subject SMTP** check box, and then type a message for **Malware found** and **No malware found**. The default messages are:

- Malware found: `[Malware Infected]`
- No malware found: `[Malware Free]`

Append Safe Stamp (SMTP & POP3)

When there is no malware detected in the mail, you have an option to append a safe stamp at the end of a message. The safe stamp insertion serves as a security confirmation to the mail recipient. The message is customizable.

Append warning if attachment exceeds size limit and is not scanned (SMTP and POP3)

When an attachment exceeds the scan size limit and is not scanned by the STM150, a warning message will be appended to the original email. Check the box and save your changes to enable.

Replace Infected Attachment with Warning Message

If the attachment in the mail is infected, the STM150 will intercept it according to the setting you configured in Email Security > Anti-Virus > Action.

You may insert a warning message to inform the mail recipient about the malware, as well as the scan actions that the STM150 has taken. The message is customizable; make sure to keep the `%VIRUSINFO%` tag as this is the place where the STM150 inserts malware information.

The following is an example of a warning message that the STM150 can insert:

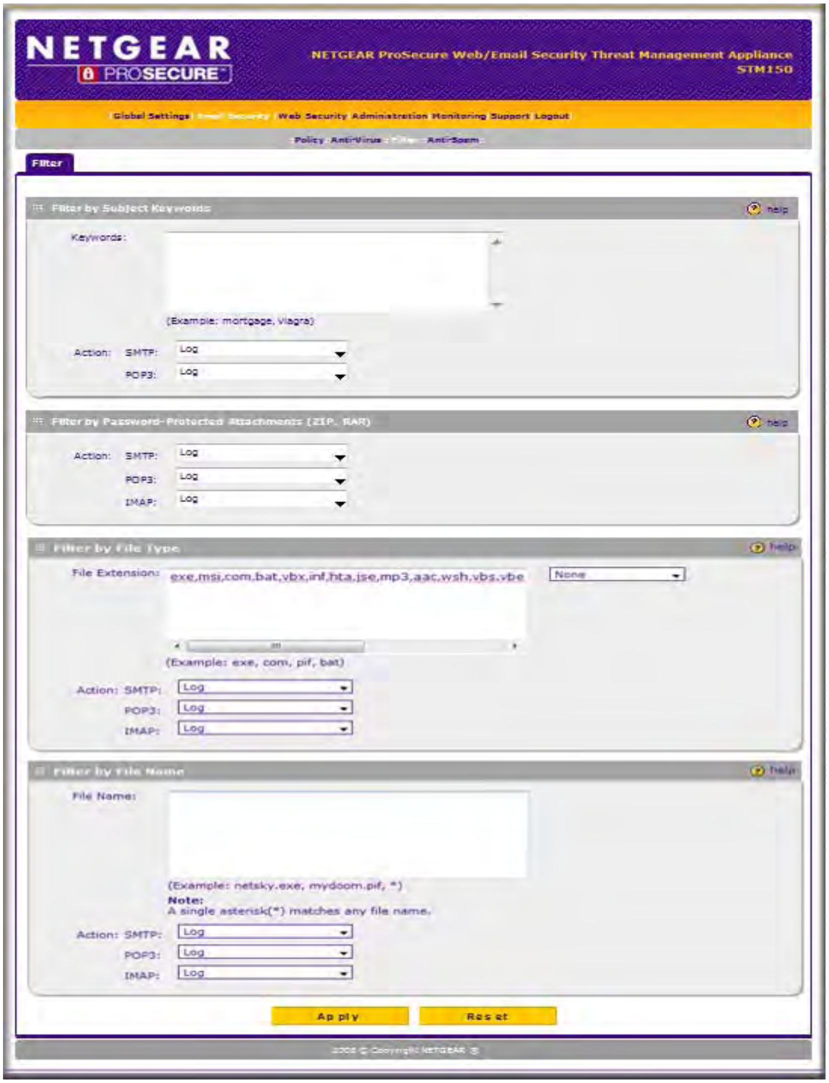
> This attachment contains malware: File 1.exe contains malware EICAR.
> Action: Delete

Send Warning Email When Malware Is Found

In addition to inserting an alert to the message, the STM150 may send out an email either to the sender, recipient, or both as notification. The subject and message body are customizable. Make sure to keep the `%VIRUSINFO%` tag so that the malware information will be inserted automatically.

Email Content Filtering

The STM150 provides several options for filtering unwanted content in the email. You can filter mails based on keywords in the subject, file type, and file name. You can also set an action to perform on emails with password-protected attachments.



Filter by Subject Keywords

Keywords:

(Example: mortgage, viagra)

Action: SMTP: Log
POP3: Log

Filter by Password-Protected Attachments (ZIP, RAR)

Action: SMTP: Log
POP3: Log
IMAP: Log

Filter by File Type

File Extension: exe,msi,com,bat,vbx,inf,hta,jse,mp3,aac,wsh,vbs,vbe None

(Example: exe, com, pif, bat)

Action: SMTP: Log
POP3: Log
IMAP: Log

Filter by File Name

File Name:

(Example: netsky.exe, mydoom.pif, *)
Note:
A single asterisk(*) matches any file name.

Action: SMTP: Log
POP3: Log
IMAP: Log

Figure 4-3

Filter by Subject Keywords

Enter the keywords to filter when they appear in the email subject line. Use commas to separate different keywords. Then select the actions for SMTP and POP3 protocols. Available filtering actions include:

- Block email & log.
- Log (default).

Filter by Password-protected Attachments

Select the actions to take for the SMTP, IMAP and POP3 protocols when a password-protected file is attached to an email. Currently, the STM150 supports blocking of password-protected ZIP and RAR files.

For SMTP, select an action the take on password protected attachments. Available actions include:

- Block attachment & log.
- Block email & log.
- Log.

For IMAP and POP3, select either **Block email & log** or **Log**.

File Extension

Enter the file extensions that you want the STM150 to filter. Use commas to separate multiple entries. For SMTP, select an action to take on the listed file extensions. Available options include:

- Block attachment & log.
- Block email & log.
- Log.

For POP3, select either **Block email & log** or **Log**.

Filter by File Type

Enter the file names that you want the STM150 to filter (for example, `netsky.exe`). Use commas to separate multiple entries. For SMTP, select an action to take on the listed file names. Available options include:

- Block attachment & log.
- Block email & log.
- Log.

For IMAP and POP3, select either **Block attachment & log** or **No Log**.

Protecting Against Email Spam

The STM150 integrates multiple anti-spam technologies to provide comprehensive protection against unwanted mail. You can enable all or a combination of these anti-spam technologies. The STM150 implements these spam prevention technologies in the following order:

1. Whitelist.
2. Blacklist.
3. Real-time blacklist.
4. Heuristic scanning.

This order of implementation ensures the optimum balance between spam prevention and system performance. For example, if a mail is originating from a whitelisted source, the STM150 will deliver the mail immediately to its destination inbox without implementing the other spam prevention technologies, thereby speeding up mail delivery and conserving the STM150 system resources. However, regardless of whether or not an email is whitelisted here, it will still be scanned by the STM150’s anti-malware engines.

You can configure these anti-spam options in conjunction with content filtering to optimize blocking of unwanted mails.

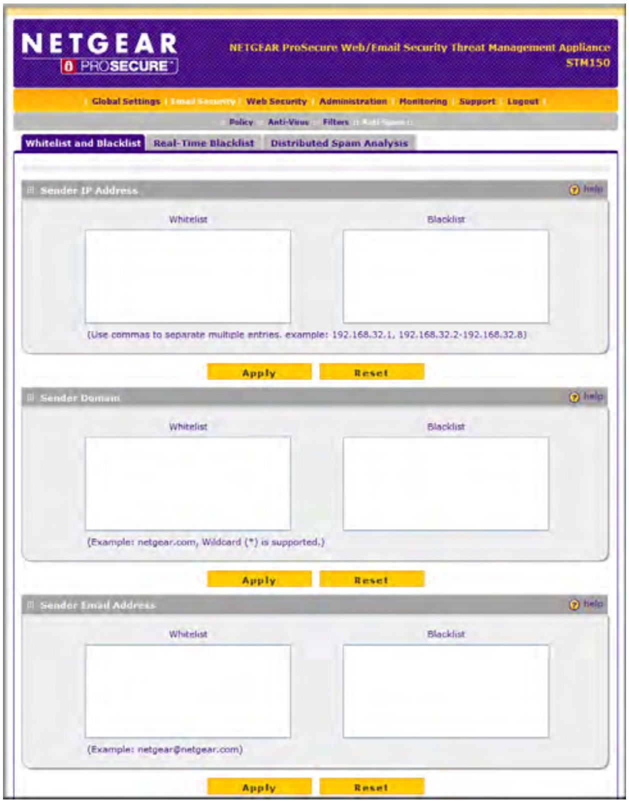
Setting Up the Whitelist and Blacklist

You can define mails that will be accepted or blocked based on the originating IP address, domain, and email address by setting up the whitelist and blacklist. You can also define mails that will be accepted based on the destination domain and email address.

The whitelist ensures that mail from listed (trusted) sources and recipients are not mistakenly tagged as spam. Mails going to and from these sources and recipients are delivered to their destinations immediately, without being scanned by the anti-spam engines. This can help speed up the system and network performance. The blacklist, on the other hand, lists sources from which all mail messages will be blocked You can enter up to 200 comma separated entries per list..

Note: The whitelist takes precedence over the blacklist, which means that if an email source is on both the blacklist and the whitelist, the email will not be scanned by the anti-spam engines.

To define the sender whitelist. On the menu, go to **Email Security** > **Anti-Spam** > **Whitelist and Blacklist**.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout
Policy : Anti-Virus : Filters :: Anti-Spam ::
Whitelist and Blacklist
Real-Time Blacklist
Distributed Spam Analysis
Sender IP Address
help
Whitelist
Blacklist
Apply
Reset
Sender Domain
help
Whitelist
Blacklist
Apply
Reset
Sender Email Address
help
Whitelist
Blacklist
Apply
Reset

(Use commas to separate multiple entries. example: 192.168.32.1, 192.168.32.2-192.168.32.8)

(Example: netgear.com, Wildcard (*) is supported.)

(Example: netgear@netgear.com)

Figure 4-4

1. Under the **Whitelist** column, enter the IP address (or IP address range), domain name, or email address that you want set as a trusted source.

   Note: Whitelist URL entries are case sensitive.

   Here are some examples:

   - IP address/IP address range: `10.1.1.5` or `10.1.2.3-35`
   - Domain name: `netgear.com`
   - Email address: `admin@netgear.com`

2. Click **Apply**.

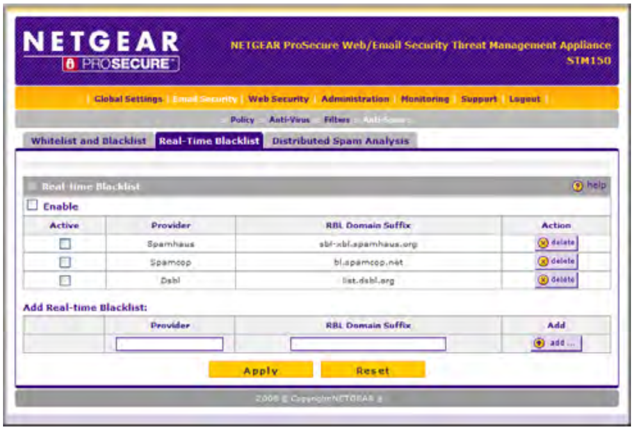
To define the recipient whitelist. On the menu, go to **Email Security >Anti-Spam** > **Whitelist and Blacklist**.

1. Under the **Whitelist** column, enter the domain name, or email address that you want set as a trusted source.
2. Click **Apply**.

To define the blacklist. **1.**Under the **Blacklist** column, enter the IP address (or IP address range), domain name, or email address that you want set as a blocked source. Click **Apply**.

Configuring the Real-time Blacklist

On the menu, go to **Email Security > Anti-Spam** > **Real-time Blacklist**.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout
Policy | Anti-Virus | Filters | Anti-Spam
Whitelist and Blacklist | Real-Time Blacklist | Distributed Spam Analysis
Real-time Blacklist
help
2008 © Copyright NETGEAR ®

□ Enable

Active	Provider	RBL Domain Suffix	Action
□	Spamhaus	sbl-xbl.spamhaus.org	delete
□	Spamcop	bl.spamcop.net	delete
□	Dsbl	list.dsbl.org	delete

Add Real-time Blacklist:

	Provider	RBL Domain Suffix	Add
			add ...

Apply | Reset

Figure 4-5

Blacklist providers are organizations that collect IP addresses of verified open SMTP relays that may be used by spammers as media for sending spam. These known spam relays are compiled by blacklist providers and are made available to the public in the form of real-time blacklists (RBLs). By accessing these RBLs, the STM150 can block spam originating from known spam sources.

By default, the STM150 comes with three pre-defined RBLs, Dsbl, Spamhaus, and Spamcop. There is no limit to the number of blacklist providers that you can add to the RBL sources.

1. Select which RBL sources you wish to enable under Active.
2. Click **Apply**.

To add a new provider.

1. In the **Add Real-time Blacklist** section, type the name of the provider under the **Provider** column.
2. Under **RBL Domain Suffix**, type the domain name from which the STM150 will retrieve the real-time blacklist.
3. Click **Add**. The message `Configuration saved` appears.

To delete a provider.

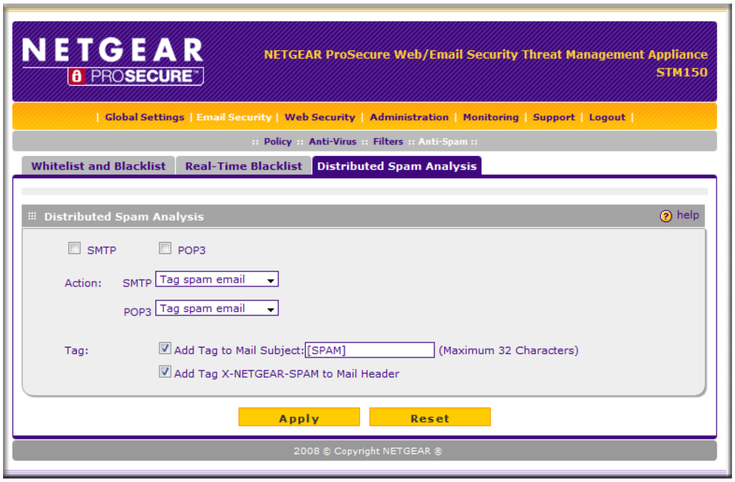
1. Select the **Active** check box for the provider that you want to delete.
2. Click **Delete** on the same row as the provider name that you want to delete. A confirmation message appears.
3. Click **OK**. The message `Configuration saved` appears.

Configuring Distributed Spam Analysis

The STM150 uses a distributed spam analysis architecture to determine whether or not an email is spam for SMTP and POP3 emails. Any email that is identified as spam will be tagged as spam (SMTP and POP3) or blocked (SMTP).

➡	**Note:** Unlike other scans, you do not configure the spam score because Netgear is doing the scoring automatically, as long as the STM is connected to the Internet.

If tag spam email is selected, the STM150 will append a spam tag (customizable) in the mail subject.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
| Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout |
:: Policy :: Anti-Virus :: Filters :: Anti-Spam ::
Whitelist and Blacklist
Real-Time Blacklist
Distributed Spam Analysis
Distributed Spam Analysis
help
Apply
Reset
2008 © Copyright NETGEAR ®

☐ SMTP ☐ POP3

Action: SMTP Tag spam email

POP3 Tag spam email

Tag: ☑ Add Tag to Mail Subject: [SPAM] (Maximum 32 Characters)

☑ Add Tag X-NETGEAR-SPAM to Mail Header

Figure 4-6

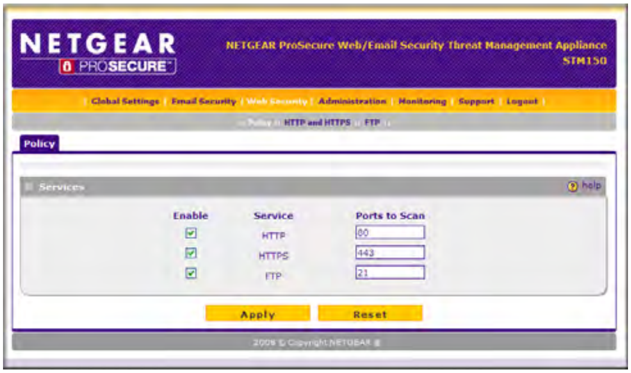
Note: For the spam analysis to function correctly, the STM150 must be connected to the Internet.

To configure distributed spam analysis.

1. On the main menu, go to **Email Security** > **Anti-Spam** > **Distributed Spam Analysis**.
2. In the Distributed Spam Analysis section, check the **SMTP** and **POP3** boxes. You can either Block spam mail or Tag spam email.
3. If you selected Tag spam email, select one of or both of the following options:
   - Add tag to mail subject: - If this is selected then you can customize the spam tag that is appended in the email subject (default is [SPAM]).
   - Add tag X-NETGEAR-SPAM to mail header
4. Click **Apply**.

Customizing Web Scanning Settings

The STM150 also scans Web or HTTP traffic for malicious content and performs the specified action, including Delete File, Clean, Audit or Streaming.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout
Policy | HTTP and HTTPS | FTP
Policy
Services
help
Apply
Reset
2008 © Copyright NETGEAR ®

Enable	Service	Ports to Scan
☑	HTTP	80
☑	HTTPS	443
☑	FTP	21

Figure 4-7

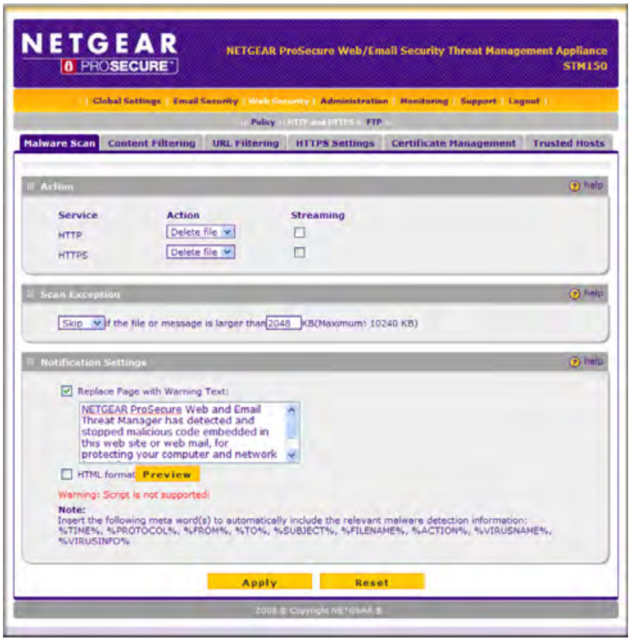
To configure Web security, go to **Web Security** > **Policy** to select which protocols to scan.

Note: Scanning all protocols enhances network security, but it may affect the performance of STM150. For an optimum balance between security and performance, only enable scanning of the most commonly used services on your network. For example, you can scan FTP and HTTP, but not HTTPS (if this last service is not often scanned).

If these services use ports other than the standard service ports (for example, port 80 for HTTP), enter these non-standard ports in under Ports to Scan. For example, if the HTTP service on your network uses both port 80 and port 8080, enter both port numbers. This will ensure that STM150 will scan traffic that is sent and received through a non-standard HTTP port.

Configuring Web Malware Scans

If you enabled HTTP or HTTPS scan in Web Security > Policy you can specify what type of action to take against detected malware.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout
Policy | HTTP and HTTPS | FTP
Malware Scan | Content Filtering | URL Filtering | HTTPS Settings | Certificate Management | Trusted Hosts
help
Apply
Reset
2008 © Copyright NETGEAR ®

Action

Service	Action	Streaming
HTTP	Delete file	□
HTTPS	Delete file	□

Scan Exception

Skip if the file or message is larger than 2048 KB(Maximum: 10240 KB)

Notification Settings

☑ Replace Page with Warning Text:

NETGEAR ProSecure Web and Email Threat Manager has detected and stopped malicious code embedded in this web site or web mail, for protecting your computer and network

□ HTML format Preview

Warning: Script is not supported!

Note:
Insert the following meta word(s) to automatically include the relevant malware detection information: %TIME%, %PROTOCOL%, %FROM%, %TO%, %SUBJECT%, %FILENAME%, %ACTION%, %VIRUSNAME%, %VIRUSINFO%

Figure 4-8

Define the action (Delete file, Log only) and check the Streaming box for each protocol you wish to enable streaming.

In Scan Exception, set the maximum file size that STM150 will scan. STM150 can scan files up to 25,600KB (25MB) in size.

Note: Setting the maximum file size to a high value may affect STM150's performance. Netgear recommends setting this value to 8,192KB (default).

In Notification Settings, you may replace a page containing malware with a warning message to inform the user about the malware, as well as the scan actions that STM150 has taken. The message is customizable; make sure to keep the %VIRUSINFO% variable as this is the place where STM150 inserts malware information.

To replace the original page with warning text. check the Replace Page with Warning Text: checkbox. Customize the warning text. If you wish to present the warning page in HTML format instead of plain text check the HTML Format checkbox. If you wish to preview the warning page in HTML format click Preview.

Click Reset to reset the page to its default settings (Action: Delete file, Streaming: off, Scan Exception value: 8,192KB).

Configuring Web Content Filtering

To configure Web filtering, go to **Web Security > HTTP and HTTPS > Content Filtering**.

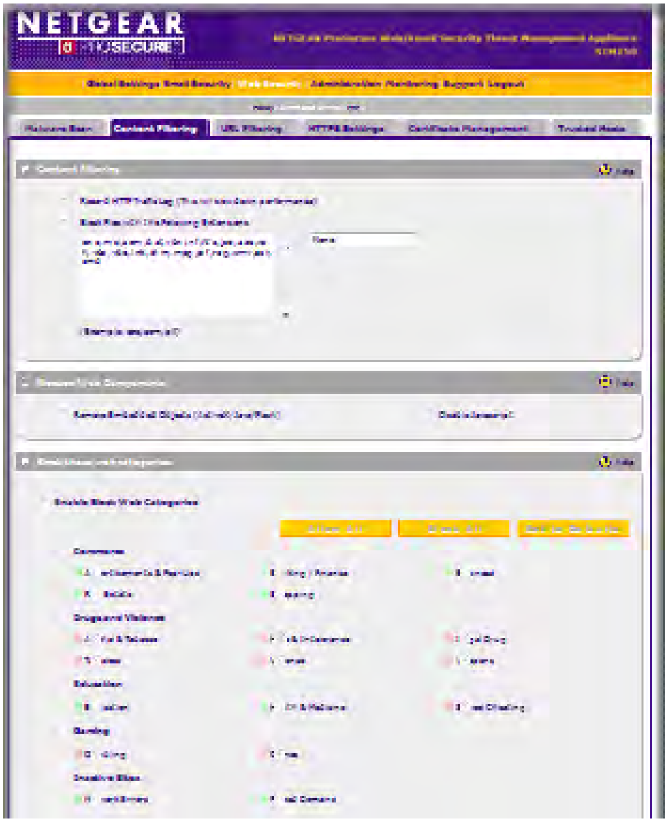


Figure 4-9

The following options are available on the Content Filtering page:

- Scan HTML Files: If you wish to scan HTML files, check the Scan HTML Files box.

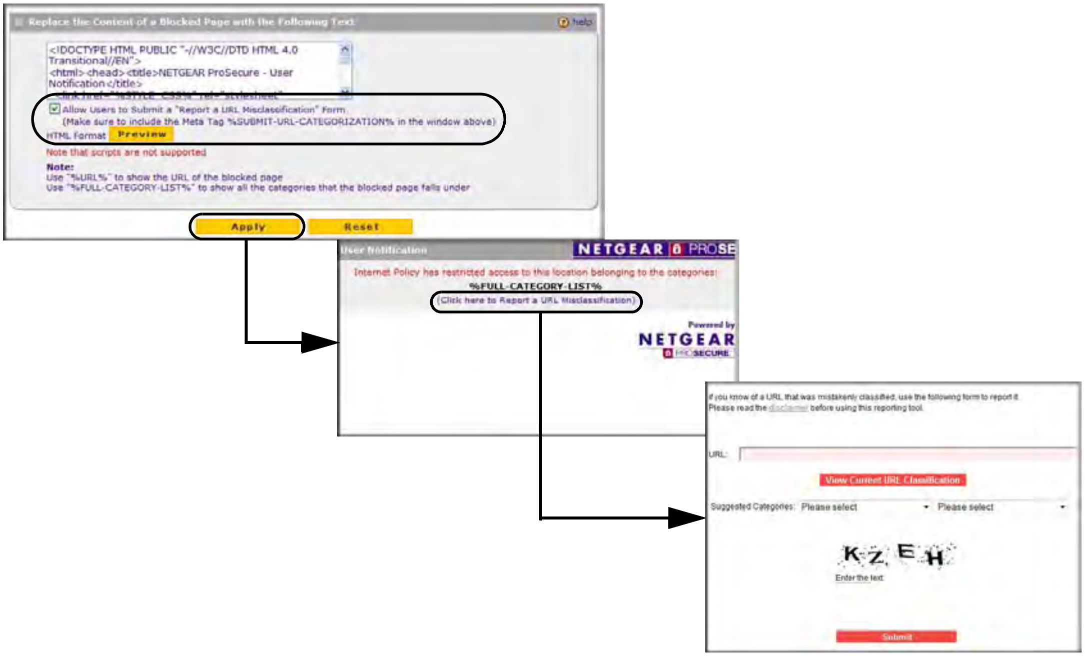
- Record HTTP traffic log: If you wish to log all scanned HTTP traffic, check the Record HTTP Traffic Log box. Keep in mind that this will slow down performance.
- Block Files with the Following Extensions: Select the Block Files with the Following Extensions checkbox.

  In the box below the Block Files with the Following Extensions check box, enter the file extensions (without the period) that you want to block. Use commas to separate multiple file extensions. The list may contain a maximum of 40 different file types. You can also add entries from a list of predefined file types. For example, if you want to block executable files, select Executables, and they will be automatically entered into the list. The predefined file types include the following:
  - Executables - exe, com, dll, so, lib, scr, bat, cmd
  - Audio and Video - wav, mp3, avi, rm, rmvb, wma, wmv, mpg, mp4, aac
  - Compressed Files - zip, rar, gz, tar, bz2
- Blocked Web Components: Select the corresponding check box to automatically block the type of web component you wish to block. Note that if any check box is selected, STM150 will block any of that type of web component that it detects, whether malicious or legitimate.
- Block these web categories: Select the check box(s) of the categories of websites you wish to block.
- Block Categories Scheduled Days: Here you can configure which days of the week you wish to enable web category blocking.

  You can select the All Days to enable web category blocking every day or select Specific Days and choose the day of week when you want to enable web category blocking.
- Block Categories Time of Day: Here you can configure which times during the day you wish to enable web category blocking.

  You can select the All Day option to enable web category blocking all times during the day. or select Specific Times option and type the time range when you wish to enable the blocking.

  Replace the Content of Blocked Pages with the Following Text: The Category and URL will be included between the two % marks. Make sure you keep the %CATEGORY% and %URL% tags while modifying the message to automatically include information about the blocked URL and which category it was in. You can preview the warning page by pressing Preview. The maximum size for the warning text message is 3 Kilobytes.



Replace the Content of a Blocked Page with the Following Text

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0
Transitional//EN">
<html><head><title>NETGEAR ProSecure - User
Notification</title>
```

☑ Allow Users to Submit a "Report a URL Misclassification" Form
(Make sure to include the Meta Tag %SUBMIT-URL-CATEGORIZATION% in the window above)

HTML Format

Note that scripts are not supported

Note:
Use "%URL%" to show the URL of the blocked page
Use "%FULL-CATEGORY-LIST%" to show all the categories that the blocked page falls under

User Notification

Internet Policy has restricted access to this location belonging to the categories:
%FULL-CATEGORY-LIST%
(Click here to Report a URL Misclassification)

If you know of a URL that was mistakenly classified, use the following form to report it.
Please read the disclaimer before using this reporting tool.

URL:

Suggested Categories: Please select Please select

Enter the text

Figure 4-10

When the STM150 blocks access to a link of a certain blocked web category, it will display an HTML warning message.

When the user clicks the Submit URL Categorization button, the STM150 will present a web form that enables the user to submit their categorization request.

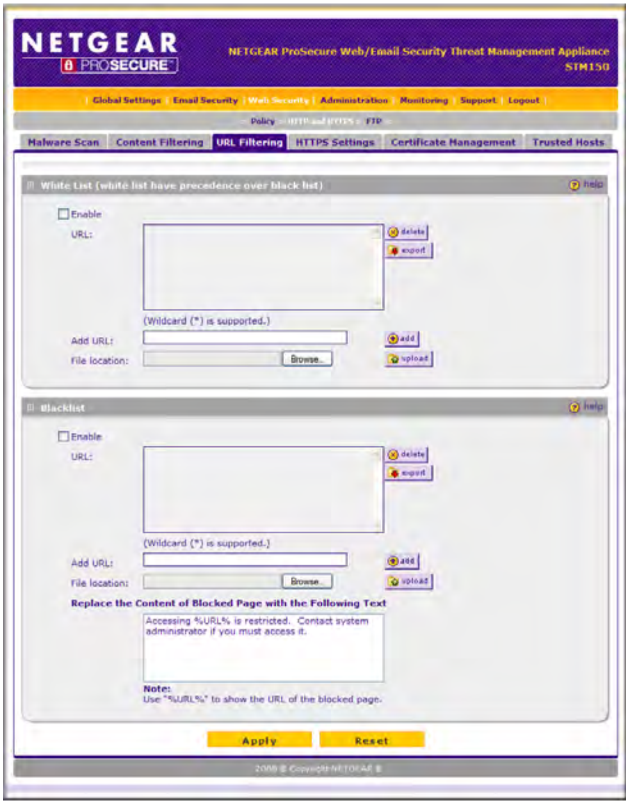
- Content Filter Lookup

  To see whether or not a certain URL has been classified by the web category filter.

  Go to **Web Security > HTTP and HTTPS> Content Filtering Lookup**. Enter the URL in the in the URL field. Click **lookup** to query the web category database.

Configuring Web URL Filtering

To configure Web filtering, go to **Web Security > HTTP and HTTPS > URL Filtering**.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
| Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout |
Policy :: HTTP and HTTPS :: FTP
Malware Scan
Content Filtering
URL Filtering
HTTPS Settings
Certificate Management
Trusted Hosts
help
delete
export
add
upload
Browse..
help
delete
export
add
upload
Browse..
Apply
Reset
2008 © Copyright NETGEAR ®

White List (white list have precedence over black list)

□ Enable

URL:

(Wildcard (*) is supported.)

Add URL:

File location:

Blacklist

□ Enable

URL:

(Wildcard (*) is supported.)

Add URL:

File location:

Replace the Content of Blocked Page with the Following Text

Accessing %URL% is restricted. Contact system administrator if you must access it.

Note:
Use "%URL%" to show the URL of the blocked page.

Figure 4-11

White List

Select the Enable check box if you want the STM150 to bypass the scanning of a URL listed here. If a URL is in both the white list and black list, then the white list will take precedence and files from the URL will not be scanned. You can enter a maximum of 200 entries to the white list.

To add a URL to the white list, enter the URLs that you want to bypass into the Add URL field, and then click add.

To delete a URL from the white list, highlight the URLs that you want to remove in the URL: field, and then click delete.

In addition to manually entering URLs one at a time, you may import and export the list. Note that the file to be imported must be in .txt format and must be line delimited (one URL per line). Use Notepad or any other text viewer to open the imported file. Click export and save the exported file to your PC. To import a list, click Browse..., Select the file you wish to import from, then click on the Open button. Click on the upload button. If the list exceeds 200 entries after the import, the import will fail.

Blacklist

Select the Enable check box if you want STM150 to block access to the sites listed here. You can enter a maximum of 200 entries to the black list.

To add a URL to the blacklist, enter the URLs that you want to block into the Add URL field, and then click add.

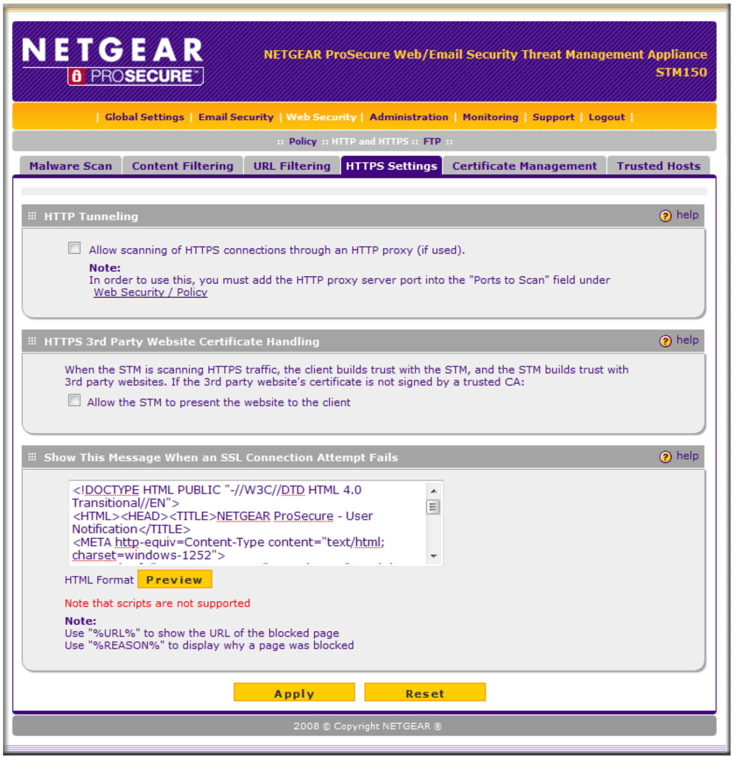
To delete a URL from the blacklist, highlight the URLs that you want to remove in the URL: field, and then click delete.

In addition to manually entering URLs one at a time, you may import and export the list. Note that the file to be imported must be in .txt format and must be line delimited (one URL per line). Use Notepad or any other text viewer to open the imported file. Click export and save the exported file to your PC. To import a list, click Browse..., Select the file you wish to import from, then click on the Open button. Click on the upload button. If the list exceeds 200 entries after the import, the import will fail.

Replace the Content of Blocked Page with the Following Text: When the STM150 blocks a page, you can display a custom warning text instead of the standard access forbidden prompt. The URL will be included between the two % marks. Make sure you keep the %URL% tag while composing the message to automatically include information about the blocked URL.

HTTPS Scan Settings

To configure the HTTPS scan settings, go to **Web Security > HTTPS Scan** > **Settings**.



NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
| Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout |
:: Policy :: HTTP and HTTPS :: FTP ::
Malware Scan
Content Filtering
URL Filtering
HTTPS Settings
Certificate Management
Trusted Hosts

HTTP Tunneling

□ Allow scanning of HTTPS connections through an HTTP proxy (if used).

Note:
In order to use this, you must add the HTTP proxy server port into the "Ports to Scan" field under Web Security / Policy

HTTPS 3rd Party Website Certificate Handling

When the STM is scanning HTTPS traffic, the client builds trust with the STM, and the STM builds trust with 3rd party websites. If the 3rd party website's certificate is not signed by a trusted CA:

□ Allow the STM to present the website to the client

Show This Message When an SSL Connection Attempt Fails

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0
Transitional//EN">
<HTML><HEAD><TITLE>NETGEAR ProSecure - User
Notification</TITLE>
<META http-equiv=Content-Type content="text/html;
charset=windows-1252">
```

HTML Format Preview

Note that scripts are not supported

Note:
Use "%URL%" to show the URL of the blocked page
Use "%REASON%" to display why a page was blocked

Figure 4-12

To configure the HTTPS scan settings, click Web Security > HTTP and HTTPS > HTTPS Settings, and set the following options.

HTTP Tunneling

Check the box to allow and scan HTTPS connections through a HTTP proxy. Be sure to add the proxy port into the Ports to Scan for the HTTPS protocol in the Policy page.

HTTPS Third Party Website Certificate Handling

In addition to the trusted certificates, you have an option to grant access to the certificates that were not signed by a trusted CA. Normally if the certificate does not satisfy all three points required, the connection will be rejected with an alert message in the browser window. To allow access, select the Allow the STM to present the website to the client. check box.

Show This Message When an SSL Connection Attempt Fails

When the STM150 denies access to an HTTPS web site, it will display an HTML warning message. The URL and reason will be included between the two % marks. Make sure you keep the %URL% and %REASON% tags while modifying the message to automatically include information about the blocked URL and the reason connection to it failed. You can preview the warning page by pressing Preview. The maximum size for the warning text message is 3 Kilobytes. Scripts are not supported.

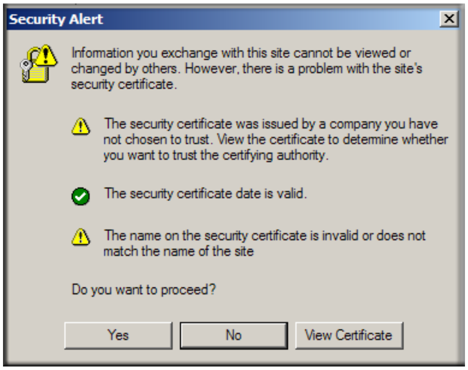
The STM150 CA Certificate

HTTPS is a secure version of HTTP used by Web sites for handling secure transactions. When the STM150 (with HTTPS scanning enabled) is located between the client and the server, the STM150 breaks the SSL connection into two parts.

1. Client <-> STM150
2. STM150 <-> Server

When the client makes a request, the STM150 will communicate with the server on its behalf. The server then returns a certificate to the STM150 for authentication. Next, the STM150 will dynamically generate and pass a certificate of its own to the client in place of the server's certificate, which means the client will see the STM150 generated certificate rather than the one from the server.

Due to the nature of HTTPS scanning and how the certificates are handled, the end user will see Security Alerts in their web browser as shown in the following figure. This is because the client (browser) will get a certificate from the STM150 instead of directly from the server.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Figure 4-13

During SSL authentication, the client authenticates three items:

- Is the certificate trusted?
- Has the certificate expired?
- Does the name on the certificate match that of the Web site?

If one of these is NOT satisfied, a security alert appears in the browser window.

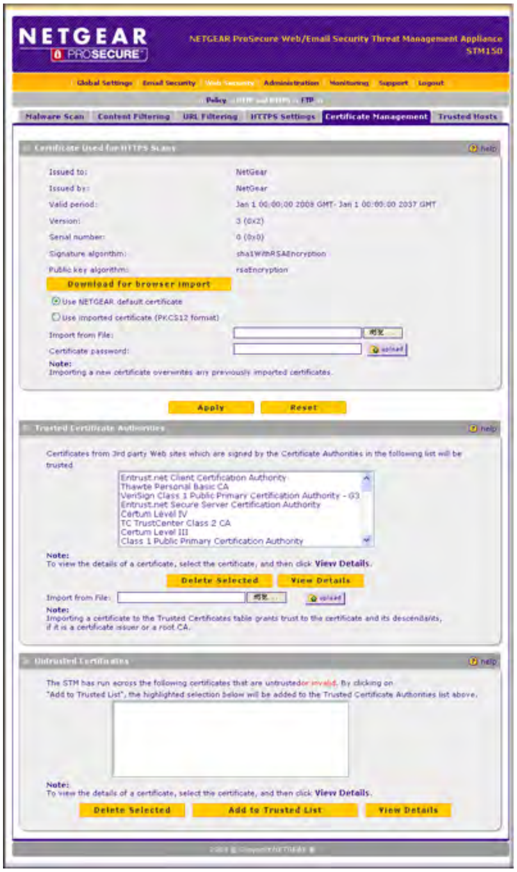
If HTTPS scan is enabled, an alert message appears when a user connected to the STM150 visits an HTTPS site. Note that this is not a bug in the STM150 – it is a result of HTTPS scanning and the way SSL works. The STM150 generated certificate has the same name and expiration date of the original certificate sent by the server. However, since the certificate was generated by the STM150 and not a trusted certificate authority, the browser will notify the user that the certificate is not valid. To prevent these popups, you must add NETGEAR as a trusted root CA in your browser.

If client authentication is required, the STM150 may not be able to scan the HTTPS traffic in some cases due to the nature of SSL. SSL has two parts – client and server authentication. Server authentication occurs with every HTTPS request, but client authentication is NOT mandatory, and rarely occurs. As a result, whether the request is from the STM150 or the real client is of less importance.

However, certain HTTPS servers do require client certificate authentication for every HTTPS request. By the design of SSL, the client needs to present its own certificate rather than using the one from the STM150. The HTTPS scanning process will be affected because of this.

Certificate Management

To manage the security certificates that you use with the STM150, go to
Web Security > **HTTPS Scan** > **Certificate Management**.



Issued to: NetGear
Issued by: NetGear
Valid period: Jan 1 00:00:00 2008 GMT- Jan 1 00:00:00 2037 GMT
Version: 3 (0x2)
Serial number: 0 (0x0)
Signature algorithm: sha1WithRSAEncryption
Public key algorithm: rsaEncryption

● Use NETGEAR default certificate
○ Use imported certificate (PKCS12 format)

Import from File:
Certificate password:

Note:
Importing a new certificate overwrites any previously imported certificates.

Certificates from 3rd party Web sites which are signed by the Certificate Authorities in the following list will be trusted

Entrust.net Client Certification Authority
Thawte Personal Basic CA
VeriSign Class 1 Public Primary Certification Authority - G3
Entrust.net Secure Server Certification Authority
Certum Level IV
TC TrustCenter Class 2 CA
Certum Level III
Class 1 Public Primary Certification Authority

Note:
To view the details of a certificate, select the certificate, and then click **View Details**.

Import from File:

Note:
Importing a certificate to the Trusted Certificates table grants trust to the certificate and its descendants, if it is a certificate issuer or a root CA.

The STM has run across the following certificates that are untrustedor invalid. By clicking on "Add to Trusted List", the highlighted selection below will be added to the Trusted Certificate Authorities list above.

Note:
To view the details of a certificate, select the certificate, and then click **View Details**.

Figure 4-14

To avoid receiving a warning prompt when visiting a site whose certificate is not trusted, you may add the certificate issuer or root CA to the trusted list.

Before enabling HTTPS scanning, you may specify which certificate to be used by the STM150 to handle HTTPS requests. By default, a certificate issued by NETGEAR is used. This certificate can be downloaded from the STM150 login screen for browser import. Click **Import** to import a certificate of your choice. A password is required for some certificates.

Note that the newly imported certificate will overwrite the existing certificate.

To import a new certificate used for HTTPS scans

1. In the Import from File field, click **Browse**, and then select the certificate file.
2. Provide the certificate password.
3. Click **Upload**.

Trusted Certificate Authorities

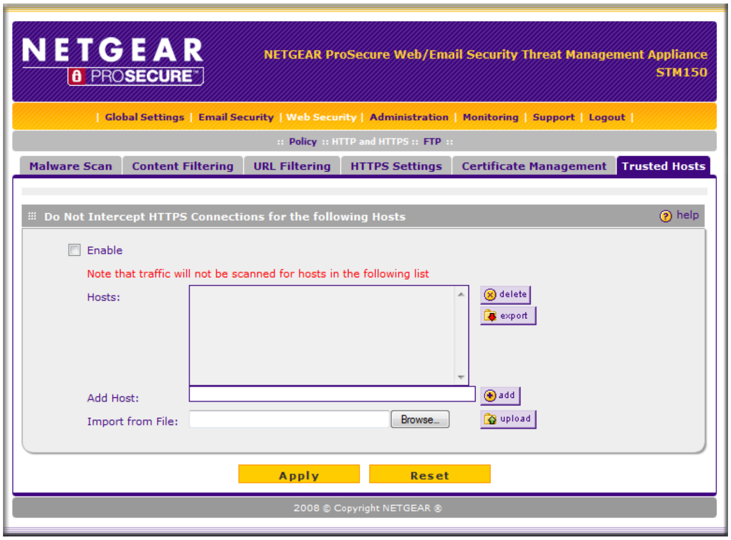
Trusted certificates are listed here. Click **Delete Selected** to delete a certificate from the trusted list. Click **View Details** to view the details of a certificate.

Untrusted Certificates

When visiting a site with a certificate that was signed by an untrusted CA, the site will automatically be listed in the Untrusted Certificates section under the Certificates Management page of the STM150 Web interface. After it is added to the list, you will have the option to add it to the STM150's trusted list, delete it from the exception list, or view the details of the certificate.

Trusted Hosts

To identify trusted hosts, go to
Web Security > HTTP and HTTPS > Trusted Hosts


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
| Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout |
:: Policy :: HTTP and HTTPS :: FTP ::
Malware Scan
Content Filtering
URL Filtering
HTTPS Settings
Certificate Management
Trusted Hosts
help
delete
export
add
Browse...
upload
Apply
Reset
2008 © Copyright NETGEAR ®

Do Not Intercept HTTPS Connections for the following Hosts

□ Enable

Note that traffic will not be scanned for hosts in the following list

Hosts:

Add Host:

Import from File:

Figure 4-15

Do Not Intercept HTTPS Connections for the Following Hosts: The STM150 will bypass the scanning and certificate authentication of the sites listed. The certificate will be sent directly to the client for authentication, which means that the user will not get a security alert for sites listed.

Note that certain sites contain elements from different HTTPS hosts. For example, if `https://example.com` contains HTTPS elements from:

- secureserver1.example.com
- secureserver2.example.com
- imageserver.example.com

You must add the above-mentioned sites to the hostlist to completely bypass the scanning of `https://example.com`. This is because different files from these three hosts are also downloaded when the user attempts to access the HTTPS page “My Page”.

To add hosts to the Host Access Control List

1. Select the **Bypass the following Hosts for HTTPS** check box to enable the bypass list.

2. Enter the host name (not the URL) of the server into the **Add Host** box, and then click **Add**. Click **Apply**.

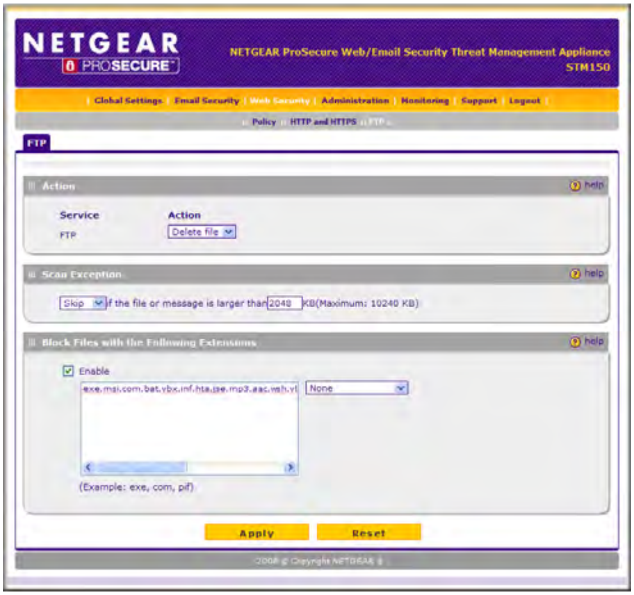
To delete hosts from the Host Access Control List

1. Select the host you wish to delete from the bypass list.
2. Click **Delete**.
3. Click **Apply**.

In addition to manually entering host names and IP addresses one at a time, you may import and export the list. Note that the files to be imported should be in .txt format, and both of the IP addresses and host names are required. Use Notepad or a similar text editor to open the exported file.

Configuring FTP Scan

To configure FTP scanning, go to
Web Security > FTP


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
| Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout |
Policy | HTTP and HTTPS | FTP
FTP
help
Apply
Reset
2008 © Copyright NETGEAR

Action

Service	Action
FTP	Delete file

Scan Exception

Skip if the file or message is larger than 2048 KB(Maximum: 10240 KB)

Block Files with the Following Extensions

☑ Enable

exe.msi.com.bat.vbx.inf.hta.jse.mp3.aac.wsh.vt | None

(Example: exe, com, pif)

Figure 4-16

If you enabled FTP scan in Web Security > Policy > FTP you can specify what type of action to take against detected malware as well as which file types to block on FTP.

Under Action you can specify what type of action to take against detected malware. You can select Delete file or Log only.

In Scan Exception, set the maximum file size that the STM150 will scan. The STM150 can scan files up to 25,600KB (25MB) in size.

Note: Setting the maximum file size to a high value may affect the STM150's performance. NETGEAR recommends setting this value to 8,192KB (default).

In Block Files with the Following Extensions, select the Enable check box.

In the box below the Enable check box, enter the file extensions (without the period) that you want to block. Use commas to separate multiple file extensions. The list may contain a maximum of 40 different file types. You can also add entries from a list of predefined file types. For example, if you want to block executable files, select Executables, and they will be automatically entered into the list. The predefined file types include the following:

- Executables - exe, com, dll, so, lib, scr, bat, cmd
- Audio and Video - wav ,mp3, avi, rm, rmvb, wma, wmv, mpg, mp4, aac
- Compressed Files - zip, rar, gz, tar, bz2

Click Reset to clear the block list and to reset the page to its default settings (Action: Delete file, Scan Exception 8,192KB).

Chapter 5
Monitoring System Performance

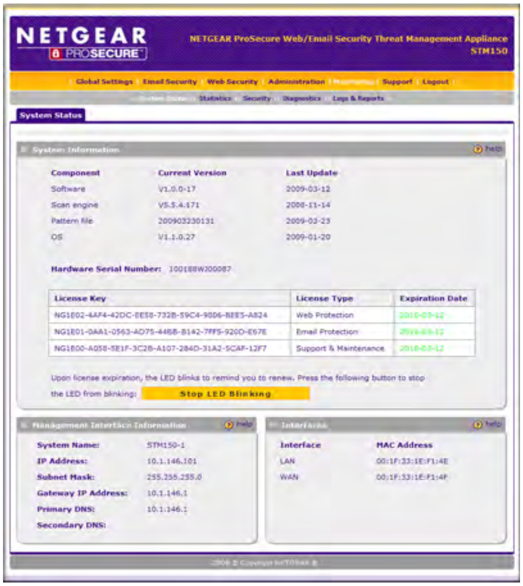
The STM150 provides online support services along with real-time alerts and comprehensive monitoring, reporting and logging capabilities to ensure that you are able to effectively respond to the latest threats found on the network.

This chapter provides information on the available logs and reports and how to view them on the Web interface. Topics discussed include:

- "Viewing the System Status" on page 5-2
- "Using Statistics and Web Usage Data" on page 5-3
- "Monitoring Security" on page 5-5
- "Running Diagnostics" on page 5-6
- "Using Reports to Optimize Protection and Performance" on page 5-8
- "Using Online Support" on page 5-12

Viewing the System Status

To view system status information, click **Monitoring** > **System Status**.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout
System Status | Statistics | Security | Diagnostics | Logs & Reports
System Status
help
Stop LED Blinking
2008 © Copyright NETGEAR ®

System Information

Component	Current Version	Last Update
Software	V1.0.0-17	2009-03-12
Scan engine	V5.5.4.171	2008-11-14
Pattern file	200903230131	2009-03-23
OS	V1.1.0.27	2009-01-20

Hardware Serial Number: 100188WJ00087

License Key	License Type	Expiration Date
NG1E02-4AF4-42DC-EE58-732B-59C4-9806-BEE5-A824	Web Protection	2010-03-12
NG1E01-0AA1-0563-AD75-4468-8142-7FF5-920D-E67E	Email Protection	2010-03-12
NG1E00-A058-5E1F-3C2B-A107-284D-31A2-5CAF-12F7	Support & Maintenance	2010-03-12

Upon license expiration, the LED blinks to remind you to renew. Press the following button to stop the LED from blinking:

Management Interface Information

System Name:	STM150-1
IP Address:	10.1.146.101
Subnet Mask:	255.255.255.0
Gateway IP Address:	10.1.146.1
Primary DNS:	10.1.146.1
Secondary DNS:	

Interfaces

Interface	MAC Address
LAN	00:1F:33:1E:F1:4E
WAN	00:1F:33:1E:F1:4F

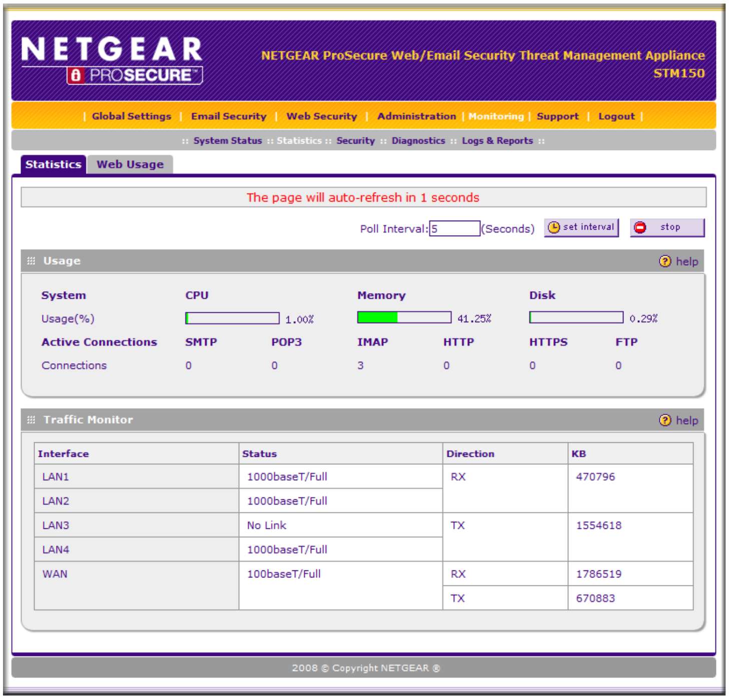
Figure 5-1

The at-a-glance table on this page allows you quickly view the status of important components of the STM150. Information available on this page includes:

- System Info - Shows component version, update information, hardware serial number and license expiration dates for each type of license.
- When a license expires, a led on the STM150 front panel will blink continuously. To stop this, click on the **Stop Led Blink** button. After this has been clicked, the button will be greyed out until the next time a license expires.
- Network - Shows the network settings of the STM150.
- Ports - Shows the MAC address for each interface on the STM150.

Using Statistics and Web Usage Data

To view system statistics, click **Monitoring** > **Statistics**.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance
STM150
| Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout |
:: System Status :: Statistics :: Security :: Diagnostics :: Logs & Reports ::
Statistics
Web Usage
set interval
stop
help
help
2008 © Copyright NETGEAR ®

The page will auto-refresh in 1 seconds

Poll Interval: 5 (Seconds)

Usage

System	CPU		Memory		Disk	
Usage(%)	1.00%		41.25%		0.29%	
Active Connections	**SMTP**	**POP3**	**IMAP**	**HTTP**	**HTTPS**	**FTP**
Connections	0	0	3	0	0	0

Traffic Monitor

Interface	Status	Direction	KB
LAN1	1000baseT/Full	RX	470796
LAN2	1000baseT/Full		
LAN3	No Link	TX	1554618
LAN4	1000baseT/Full		
WAN	100baseT/Full	RX	1786519
		TX	670883

Figure 5-2

The at-a-glance table on the Statistics tab page lets you review the distribution of traffic going through this STM150. Information available on this page includes:

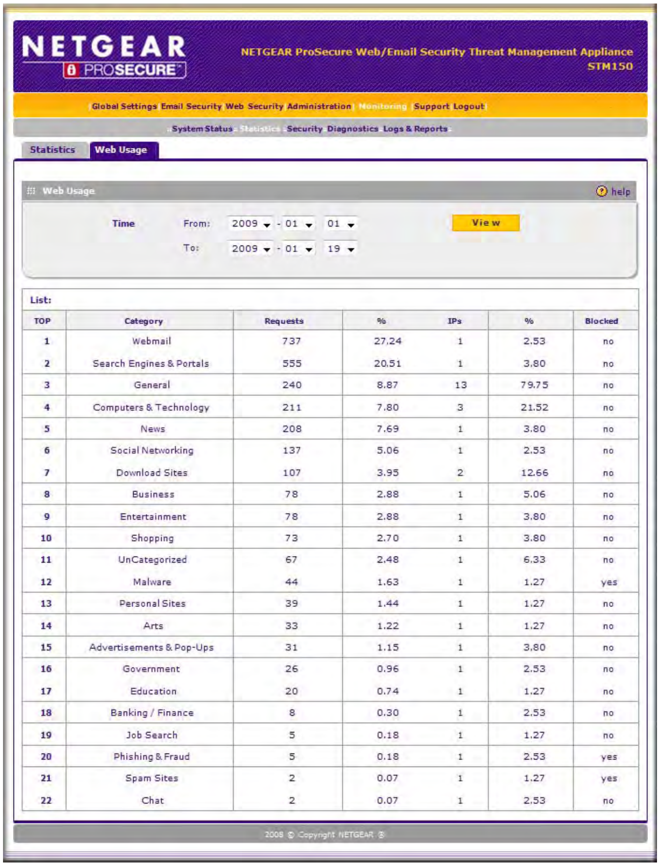
Usage - Shows CPU, memory, and disk space usage

Active Connections - Shows the number active connections for each supported protocol

Traffic Monitor - Shows the status of each network interface and the volume of incoming and outgoing traffic for each interface

To change how often the page refreshes, enter the desired refresh interval in the **Poll Interval** field and click the **Set Interval** button. To stop the page from refreshing, click the **Stop** button.

To view Web usage statistics, click **Monitoring** > **Statistics** >**Web Usage**.



Time From: 2009 - 01 01

To: 2009 - 01 19

List:

TOP	Category	Requests	%	IPs	%	Blocked
1	Webmail	737	27.24	1	2.53	no
2	Search Engines & Portals	555	20.51	1	3.80	no
3	General	240	8.87	13	79.75	no
4	Computers & Technology	211	7.80	3	21.52	no
5	News	208	7.69	1	3.80	no
6	Social Networking	137	5.06	1	2.53	no
7	Download Sites	107	3.95	2	12.66	no
8	Business	78	2.88	1	5.06	no
9	Entertainment	78	2.88	1	3.80	no
10	Shopping	73	2.70	1	3.80	no
11	UnCategorized	67	2.48	1	6.33	no
12	Malware	44	1.63	1	1.27	yes
13	Personal Sites	39	1.44	1	1.27	no
14	Arts	33	1.22	1	1.27	no
15	Advertisements & Pop-Ups	31	1.15	1	3.80	no
16	Government	26	0.96	1	2.53	no
17	Education	20	0.74	1	1.27	no
18	Banking / Finance	8	0.30	1	2.53	no
19	Job Search	5	0.18	1	1.27	no
20	Phishing & Fraud	5	0.18	1	2.53	yes
21	Spam Sites	2	0.07	1	1.27	yes
22	Chat	2	0.07	1	2.53	no

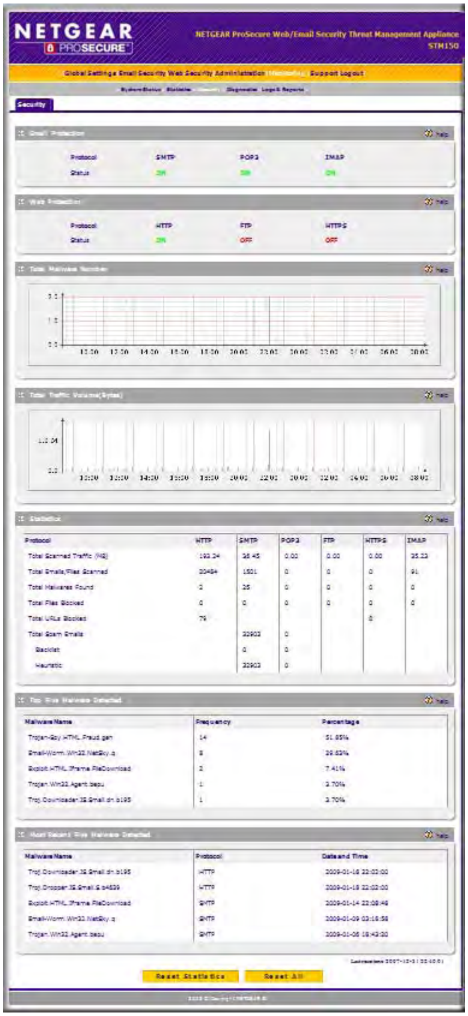
Figure 5-3

Select the time frame for the Web Usage report then click **View**

The at-a-glance table on this page allows you to quickly see which categories of Web sites are getting the most access from your network.

Monitoring Security

To view a summary of malware incidents on the network, click **Monitoring** > **Security.**


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
Global Settings Email Security Web Security Administration Monitoring Support Logout
System Status Statistics Security Diagnostics Logs & Reports
Security
help
Total Malware Number
2.0
1.0
0.0
12:00 13:00 14:00 15:00 18:00 20:02 22:02 20:02 22:02 24:02 26:02 28:02
Total Traffic Volume(Bytes)
1.0 04
0.0
Reset Statistics
Reset All

Email Protection

Protocol	SMTP	POP3	IMAP
Status	ON	ON	ON

Web Protection

Protocol	HTTP	FTP	HTTPS
Status	ON	OFF	OFF

Statistics

Protocol	HTTP	SMTP	POP3	FTP	HTTPS	IMAP
Total Scanned Traffic (MB)	193.24	38.45	0.00	0.00	0.00	35.23
Total Emails/Files Scanned	20494	1501	0	0	0	91
Total Malwares Found	2	25	0	0	0	0
Total Files Blocked	0	0	0	0	0	0
Total URLs Blocked	79				0	
Total Spam Emails		32903	0			
Blacklist		0	0			
Heuristic		32903	0			

Top Five Malware Detected

Malware Name	Frequency	Percentage
Trojan-Spy.HTML.Fraud.gen	14	51.85%
Email-Worm.Win32.NetSky.q	8	29.63%
Exploit.HTML.IFrame.FileDownload	2	7.41%
Trojan.Win32.Agent.bepu	1	3.70%
Troj.Downloader.JS.Small.dn.b195	1	3.70%

Most Recent Five Malware Detected

Malware Name	Protocol	Date and Time
Troj.Downloader.JS.Small.dn.b195	HTTP	2009-01-18 22:02:00
Troj.Dropper.JS.Small.g.b4639	HTTP	2009-01-18 22:02:00
Exploit.HTML.IFrame.FileDownload	SMTP	2009-01-14 22:08:46
Email-Worm.Win32.NetSky.q	SMTP	2009-01-09 03:16:58
Trojan.Win32.Agent.bepu	SMTP	2009-01-06 18:43:30

Last update 2007-12-31 22:40:01

Figure 5-4

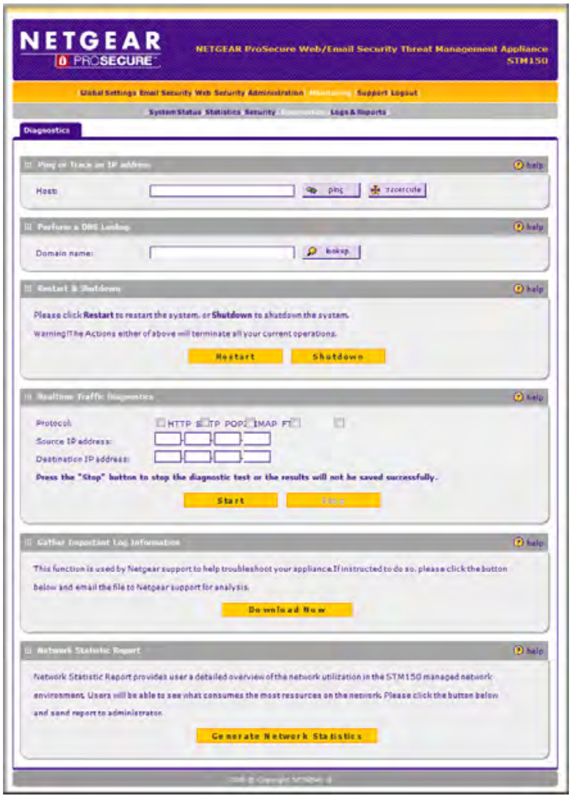
Spam and malware detected on the SMTP, IMAP, POP3, HTTP, HTTPS and FTP protocols are listed on this page, in addition to the actions taken on the malicious code. The status of the scanning services are also shown here as well. The five most frequently detected malware are listed (ranked) here, as well as the five most recently detected malware (listed chronologically).

Running Diagnostics

The STM150 provides diagnostic tools that help you analyze traffic conditions and the status of the network. Two sets of tools are available – network diagnostic tools and traffic diagnostic tools. Network diagnostic tools provide PING and DNS lookup, while traffic diagnostic tools allow you to perform real-time, per-protocol traffic analysis between specific source and destination addresses as well as the ability to generate reports on network usage in your network.

Using the Network Diagnostic Tools

To use the network diagnostic tools, go to
Monitoring > Diagnostics


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
Global Settings Email Security Web Security Administration Monitoring Support Logout
System Status Statistics Security Diagnostics Logs & Reports
Diagnostics
Ping or Trace an IP address
help
Host
ping
traceroute
Perform a DNS Lookup
Domain name:
lookup
Restart & Shutdown
Restart
Shutdown
Realtime Traffic Diagnostics
Protocol:
HTTP SMTP POP3 IMAP FTP
Source IP address:
Destination IP address:
Start
Stop
Gather Important Log Information
Download Now
Network Statistic Report
Generate Network Statistics

Please click **Restart** to restart the system. or **Shutdown** to shutdown the system.

Warning!The Actions either of above will terminate all your current operations.

Press the "Stop" button to stop the diagnostic test or the results will not be saved successfully.

This function is used by Netgear support to help troubleshoot your appliance.If instructed to do so. please click the button below and email the file to Netgear support for analysis.

Network Statistic Report provides user a detailed overview of the network utilization in the STM150 managed network environment. Users will be able to see what consumes the most resources on the network. Please click the button below and send report to administrator.

Figure 5-5

Use PING to check the connection between the STM150 and a specific IP address. Enter the IP address or host name, and then click PING. The PING results appear at the bottom of the page.

To perform DNS lookup, enter the domain name, and then click DNS Lookup. The page refreshes, and then the DNS lookup results (domain name and IP addresses) appear at the bottom of the page.

Click Restart or Shutdown to restart or shutdown the system, which terminates all sessions.

Using the Realtime Traffic Diagnostic Tools

1. In **Protocol**, select the protocols that you want to analyze. You can select a single or a combination of protocols.
2. In **Source IP address**, enter the origin of traffic that you want to analyze.
3. In **Destination IP address**, enter the target host for which the traffic is intended.
4. Click **Start**. You will be prompted to save the downloaded traffic capture to your PC.
5. Select a location to save the file and click OK. A file download will begin.
6. Once you are done, click **Stop**. The file download will now be complete.
7. Open the file in a network traffic analyzer tool such as Wireshark.

Gathering Important Log Information

When you request support, NETGEAR Technical Support may ask you to collect the debug logs and other information from your STM150 appliance. Use the **Gather Important Log Information** section to export information that can help NETGEAR troubleshoot the appliance.

To collect information about your STM150

1. On the Diagnostics page, click **Download Now** under the **Gather Important Log Information** section. A pop-up message appears, prompting you to confirm that you want to download the information file from the STM150. The default file name is **importantlog.gpg**
2. Select a download location for the file, and then click **OK**. Your browser downloads the information file to the location you specified.
3. When download is complete, browse to the download location you specified and verify that the file has been downloaded successfully.

Generate Network Statistics Report

The Network Statistic Report provides the user a detailed overview of the network utilization in the STM150 managed network environment. Users will be able to see what consumes the most resources on the network.

On the Monitoring > Diagnostics page, click **Generate Network Statistics** to send the report to the administrator.

Using Reports to Optimize Protection and Performance

- Working with Logs
- Working with Reports

Working with Logs

The STM150 generates logs that provide detailed information about malware and traffic activities on the network. You can view these logs on the Web interface, save the log records in CSV format, or have them automatically mailed to you.

Six types of logs are available:

- System logs
- Traffic logs
- Malware logs
- Spam logs
- Content filter logs
- Email filter logs

You can generate (or query) each log type separately and filter the information based on a number of criteria. Malware logs, for example, can be filtered using the following criteria (other log types have similar filtering criteria):

- Date range
- Protocols
- Malware name
- Action
- Client and server IP addresses

Querying Logs

System logs have their own page on the Web interface. Use the following procedure to generate the other log types.

1. To query logs, go to **Logs & Reports** > **Log Query**.
2. In **Log Type**, select the log type that you want to generate.
3. Set the filtering criteria by specifying the date range, protocol, source or destination IP address, or scan action. If you do not set the filtering criteria, all available logs for the selected log type will be displayed.
4. Click **Search**.

Log records that match the criteria you specified are displayed on the Web interface. If you want to save and download the log records to a CSV or HTML file, select the format you wish to download and click **Download**.

Sending Logs

The STM150 can send logs via email and to a syslog server on the network. You can configure both log sending methods by clicking **Log & Reports** > **Email & Syslog**.

To configure the STM150 to forward logs to a syslog server.

1. Select the **Enable** check box.
2. In **IP Address**, type the IP address of the syslog server.
3. In **Port**, type the port number that the syslog server uses to receive logs.
4. Select the check boxes for the log information that you want to forward to the syslog server. For example, if you want malware and spam logs to be sent, select the **Malware logs** and **Spam logs** check boxes.
5. For each log type that you selected, select the facility to use and assign a priority level.
6. Click **Apply**.

To email logs.

1. Select the **Enable** check box.
2. On the Log Query page, select the type of log to.
3. In **Send to**, type the email address of the log recipient.
4. In **Frequency**, specify when you want the STM150 to email logs.

5. In **Select logs to send**, select the check boxes for the log types that you want the STM150 to send via email.
6. In **Format**, click either **Plain Text** or **CSV**. If you want the STM150 to compress the log file before sending, select the **Zip the logs to save space** check box.
7. In Size, select the **Split log size to**: box and enter a file size (in Megabytes) to split the logs into fragments of the file size entered.
8. Click **Apply**.

   The STM150 will email the selected logs based on the schedule you specified. If you want the STM150 to email available logs immediately, click the **Send Now** button (located next to the **Send to** text box).

Using Logs to Identify Infected Clients

In addition to identifying malware that has been detected on the network, you can also use the STM150 logs to help identify potentially infected clients on the network. Clients that are sending out abnormally high volumes of HTTP traffic, for example, indicate possible spyware infection.

To identify infected clients that are sending spyware in the outbound traffic, query the STM150 malware logs and see if any of your internal IP addresses are the source of spyware detected at the Internet gateway. Clients generating abnormally high amounts of HTTP traffic may also be infected by spyware or other malware.

To query log data that will show this information.

1. On the Log Query page, select **Traffic** as the log type.
2. Check the **HTTP** check box, and then run the query.
3. On the traffic logs result page, click the **Size (Byte)** column heading to sort the results in a descending order.
4. Check if there are clients that are sending out suspicious volumes of data, especially to the same destination IP address, on a regular basis.

If you find a client exhibiting this behavior, you can run a query on that client's HTTP traffic activities to get more information. Do this by running the same HTTP traffic query and entering the client IP address in the **Source IP** text box.

Log Management

Generated logs take up space and resources on the STM150 disk. To ensure that there is always sufficient space to save newer logs, the STM150 automatically deletes older logs whenever the total log size reaches 50% of the allocated file size for each log type.

This automated log purging takes the burden of managing the size of the STM150 logs off your shoulders and ensures that the latest malware incidents and traffic activities are always recorded.

To manually purge selected logs, go to **Logs & Reports > Log Management** and select the check boxes under **Clear the following log information** for the logs you wish to purge, then click the **Clear Log Information** button.

Working with Reports

The STM150 provides comprehensive reporting features that enable you to view malware activities on different protocols and the types and volume of traffic entering and leaving the network. The STM150 reports provide the following information:

- Real-Time Traffic Summary – Shows a graph that indicates the traffic volume for the selected protocols during the report period, the total number of malware instances detected, and the type of malware/method used to block the malware
- Top Five Malware Detected – Shows the five malware with the highest infection count on the network
- Five Most Recent Malware Detected – Shows the last five malware detected on the network
- Malware Outbreak Alert – Shows any outbreak alerts that have been sent out during the report period
- Protocol-specific Malware Incidents and Traffic Volume – Shows graphs that illustrate the traffic volume and malware incidents during the report period

Send Reports by Email

To specify a recipient(s) to receive the STM150 reports, go to **Logs & Reports > Scheduled Report** and enter the recipient’s email address in the field provided. Check the **Frequency** box to enable report delivery and set a frequency to automatically send reports at the specified times. You can also send a report manually at any time by clicking the **Send Now** button.

To save reports.

1. On the menu, click **Logs & Reports > Scheduled Report**.
2. Select the frequency you want the STM150 to save reports (**Monthly**, **Weekly**, or **Daily**).
3. Select the maximum number of reports you want the STM150 to save on the appliance (the maximum number of reports is 12).

To download saved reports.

Click the **Download** button next to a previously saved report to download it to your PC.

To delete saved reports.

Click the **Delete** button next to a previously saved report to delete it from the STM150.

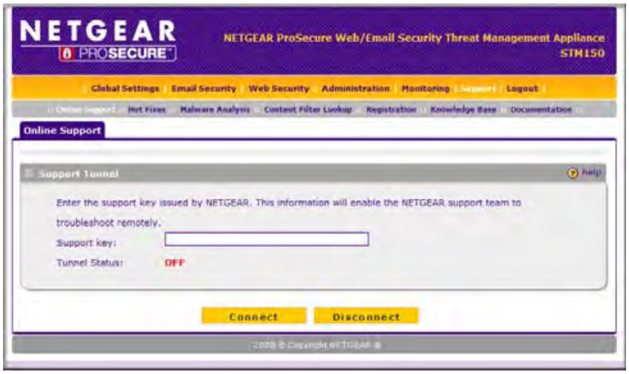
Using Online Support

Online support includes:

- Remote Troubleshooting
- Hot Fixes
- Malware Analysis
- Content Filtering

Enabling Remote Troubleshooting

To enable remote troubleshooting, go to
Support > Online Support



Enter the support key issued by NETGEAR. This information will enable the NETGEAR support team to troubleshoot remotely.

Support key:

Tunnel Status: OFF

Figure 5-6

One of the advanced features that STM150 provides is online support through the support tunnel. With this feature, NETGEAR support staff is able to analyze any difficulty you are experiencing from a remote location. Make sure that ports 443 and 2222 are open on your firewall, and you have the support key on hand.

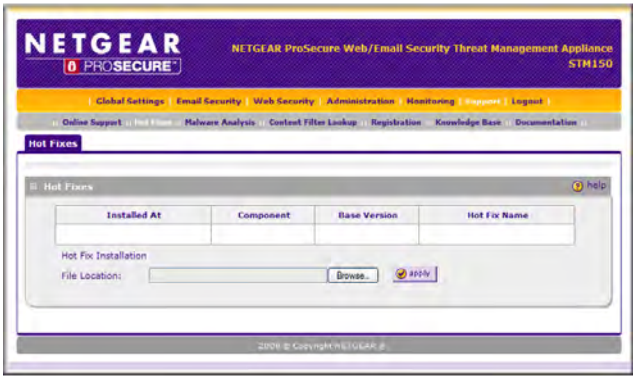
Copy and paste the support key given to you by Netgear into the Support Key field, and then click the Connect button. If the status shows the tunnel status is on, Netgear's support staff will be able to access your STM150 and perform advanced diagnostics.

If NETGEAR support cannot access your the STM150 remotely, you may be asked to save a log file to your computer and then email it to NETGEAR for analysis. If asked to do so, log into the STM150 Web interface, go to **Monitoring** > **Diagnostics** > **Gather Important Log Information** and click **Download Now**. Save the file to a local hard drive and send it by email to NETGEAR support for analysis.

Working with Hot Fixes

Netgear may release hot fixes or patches if certain problems are found in any software release. Whenever a hot fix is available, install it immediately to ensure optimum performance of your STM150 appliance. Hot fixes may be released through NETGEAR resellers or on the NETGEAR Web site.

The details of installed Hot Fixs are displayed on the **Support** > **Hot Fixes** page:


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance STM150
Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout
Online Support | Hot Fixes | Malware Analysis | Content Filter Lookup | Registration | Knowledge Base | Documentation
Hot Fixes
Hot Fixes
help
Browse...
apply
2009 © Copyright NETGEAR ®

Installed At	Component	Base Version	Hot Fix Name

Hot Fix Installation

File Location:

Figure 5-7

- Installed At - The date and time in which the hot fix was installed into the system.
- Component - The component in which the hot fix patches.
- Base Version - The base software version for a particular hot fix.
- Hot Fix Name - The name of the hot fix.

To install a hot fix:

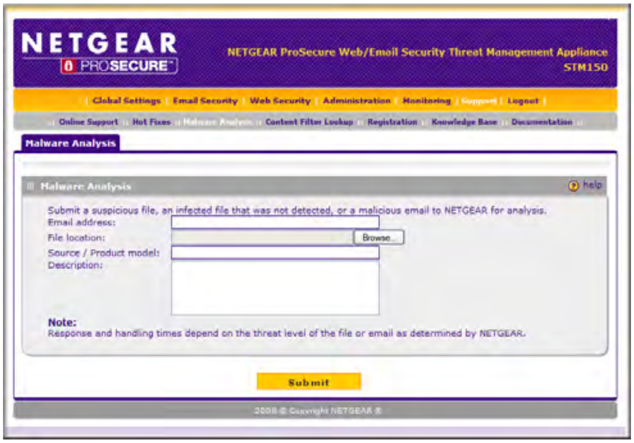
1. Obtain the hot fix from Netgear or its authorized reseller.
2. Save the hot fix file on the computer that you are using to access the STM150 Web interface.
3. Log on.
4. Go to **Support** > **Hot Fixes**.

5. Browse to the location where you saved the hot fix file, and then select it.
6. Click Open.
7. Click Apply to install the hot fix.

Sending Suspicious Files to NETGEAR for Analysis

You can report any undetected malware file or malicious email to Netgear for online for analysis. The file will be compressed and password protected before sending.

On the menu, go to **Support** > **Malware Analysis**.


NETGEAR
PROSECURE
NETGEAR ProSecure Web/Email Security Threat Management Appliance
STM150
Global Settings | Email Security | Web Security | Administration | Monitoring | Support | Logout
Online Support | Hot Fixes | Malware Analysis | Content Filter Lookup | Registration | Knowledge Base | Documentation
Malware Analysis
Malware Analysis
help
Browse...
Submit
2008 © Copyright NETGEAR ®

Submit a suspicious file, an infected file that was not detected, or a malicious email to NETGEAR for analysis.

Email address:

File location:

Source / Product model:

Description:

Note:
Response and handling times depend on the threat level of the file or email as determined by NETGEAR.

Figure 5-8

In Email address, type your email address. Browse to the infected file or mail that you want to send to Netgear for analysis. In Source / product model, indicate where the file originated (for example, an email address if received via email) or which product or scan feature (for example, Email or Web Scan) detected the file, if known. In Description (optional), type a description for the file that you are sending (if any). Click **Submit**.

Appendix A
Default Settings and Technical Specifications

You can use the reset button located on the rear panel to reset all settings to their factory defaults.

- To perform a hard reset, press and hold the reset button for approximately 10 seconds (until the TEST LED blinks rapidly). Your device will return to the factory configuration settings shown in Table A-2 below.
- Pressing the reset button for a shorter period of time will simply cause your device to reboot.

Table A-1. STM150 Default Configuration Settings

Feature		Default
Login		
	User Login URL	https://192.168.1.201
	Admin User Name (case sensitive)	admin
	Admin Login Password (case sensitive)	password
	Guest User Name (case sensitive)	guest
	Guest Login Password (case sensitive)	guest
Management		
	System Configuration	Web-based configuration and status monitoring
	Required Minimum Browser versions	Internet Explorer 5.0 or higher or Mozilla Firefox 1.0 or higher **Note**: When the unit scans secure HTTPS traffic, you must import the root CA certificate into your browser from the STM150 login screen.
	Time Zone	GMT
	Time Adjusted for Daylight Saving Time	Disabled
	SNMP	Disabled
	Remote Management	Disabled
	Administration Console Port	RS232

Table A-1. STM150 Default Configuration Settings (continued)

Feature		Default
LAN Connections		
	MAC Address	Default address
	MTU Size	1500
	Ports	5 AutoSense 10/100/1000BASE-T, RJ-45
	LAN IP Address	In line transparent bridged
	Subnet Mask	255.255.255.0

The STM150 specifications are listed in the table below.

Table A-2. STM150 Specifications

Feature		Specification
Supported Protocols		
	Data Protocols:	HTTP, HTTPS, FTP, IMAP, POP3, SMTP
Power		
	Worldwide:	100-240V AC/50-60 Hz, universal input, 1.5 A max
Physical Specifications		
	Dimensions:	43.5 x 258 x 440 mm (1.7 x 10.2 x 17.3 in.)
	Weight:	3.68 kg (8.1 lb)
Environmental Specifications		
	Operating temperature:	0° to 40° C (32º to 104º F)
	Storage temperature:	-20º to 70º C (-4º to 70º F)
	Operating humidity:	5-90% maximum relative humidity, non condensing
	Meets requirements of:	RoHS
Electromagnetic Emissions		
	Meets requirements of:	FCC Part 15 Class A
		VCCI Class A
		CE mark, commercial
Safety		
	Meets requirements of:	UL listed; C-Tick

Appendix B
Related Documents

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
Internet Networking and TCP/IP Addressing:	*http://documentation.netgear.com/reference/enu/tcpip/index.htm*
Wireless Communications:	*http://documentation.netgear.com/reference/enu/wireless/index.htm*
Preparing a Computer for Network Access:	*http://documentation.netgear.com/reference/enu/wsdhcp/index.htm*
Virtual Private Networking (VPN):	*http://documentation.netgear.com/reference/enu/vpn/index.htm*
Glossary	*http://documentation.netgear.com/reference/enu/glossary/index.htm*

Index